

# **JAUNT Information Technology Operations Manual**



**JAUNT, Inc.**

**104 Keystone Place  
Charlottesville, VA 22902**

**434-296-3184**

**fax 296-4269**

**netadmin@ridejaunt.org**

**[www.ridejaunt.org](http://www.ridejaunt.org)**

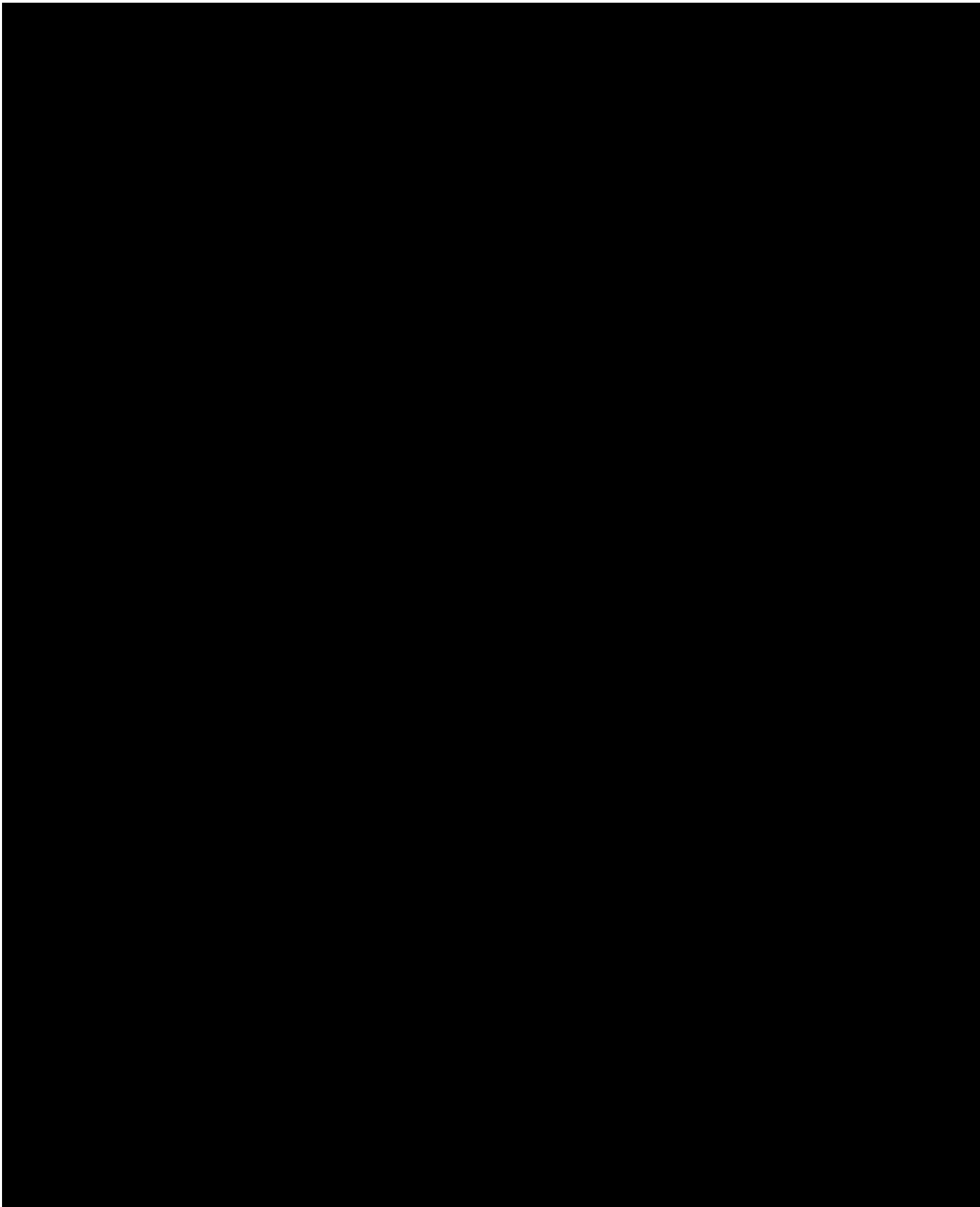
# TABLE OF CONTENTS

1.	JAUNT Network & Mobile Data Configuration Diagrams .....	5
2.	Important Contact Information .....	8
3.	Equipment Maintenance .....	11
3.1.	Servers .....	11
3.2.	PC's .....	11
3.3.	Other Equipment .....	11
4.	Software Maintenance .....	11
5.	Security .....	12
5.1.	Facilities .....	13
5.1.1.	Building .....	13
5.1.2.	Server Room, etc. ....	13
5.2.	Software & Hardware .....	13
5.2.1.	Active Directory .....	13
5.2.1.1.	Users .....	14
5.2.2.	Exchange Email .....	14
5.2.3.	Servers .....	14
5.2.4.	Desktop Computer Policy .....	15
5.2.5.	Router .....	15
5.2.6.	Users' Data .....	15
5.3.	Audits .....	16
5.4.	Intellectual Property .....	16
5.5.	Clean Up Policy .....	16
5.5.1.	Employees Leaving the Organization .....	16
5.5.2.	Equipment Disposal .....	17
6.	JAUNT Disaster Recovery Information .....	17
6.1.	Business Continuity Plan .....	17
6.1.1.	Priority of Systems .....	18
6.1.1.1.	Mission Critical .....	18
6.1.1.2.	Important .....	19
6.1.1.3.	Minor .....	19
6.1.2.	Scenarios .....	19
6.2.	Backup Operations & Procedures .....	21
6.2.1.	Recovery .....	23
6.2.2.	Backup Responsibilities .....	24
6.2.3.	Recommended Tape Storage .....	25
6.2.4.	Changing the Tape .....	25
6.2.5.	Cleaning the Tape Unit .....	26
6.2.6.	Restoring Data .....	26
6.2.7.	How to Backup and Restore the Registry .....	27
6.2.8.	Returning to the Last Known Good Menu .....	28
6.2.9.	Methods for Restoring Replicated Domain Data .....	30
	Table 1. Use the appropriate restore method for each type of replicated data. ....	31
	Table 3. How to handle server services when performing a restore .....	31
6.2.10.	FLOWCHART FOR SYSTEM RESTORATION .....	32
6.3.	XGate 3.1 – Backup Procedure .....	34
	Summary 34	
6.3.1.	Creating a Backup of the SQL Database (.XDB File) .....	34
6.3.2.	Restoring a SQL Database From an .XDB File .....	37

6.3.3.	System State Backup .....	37
6.4.	Backup Exec vs. 9.X – Software Installation Codes .....	37
6.4.1.	Veritas Disaster Recovery Links.....	38
7.	Equipment Configurations .....	38
7.1.	Servers .....	38
7.1.1.	ROOT .....	<b>Error! Bookmark not defined.</b>
7.1.2.	MANAGEMENT .....	<b>Error! Bookmark not defined.</b>
7.1.3.	EJAUNT.....	<b>Error! Bookmark not defined.</b>
7.1.4.	MANAGER .....	<b>Error! Bookmark not defined.</b>
7.1.5.	TRAPSOFT .....	38
7.1.6.	TRAPDB.....	39
7.1.7.	MDTAVL.....	39
7.1.8.	XGATE .....	39
7.1.9.	IVR1.....	40
7.1.10.	IVR2.....	40
7.1.11.	COMM .....	41
7.1.12.	HVAC.....	41
7.1.13.	MANAGEMENT .....	41
7.2.	PC Configurations .....	42
7.3.	Firewall, CSU/DSU & Router - CISCO PIX Configuration.....	42
7.4.	Phone System - ESI .....	42
7.4.1.	How to Use.....	43
7.4.1.1.	Conference Call.....	43
7.4.2.	Programming .....	43
7.4.3.	Day Mode Diagram - Including Details .....	47
7.4.4.	Night Mode Diagram.....	48
7.4.5.	Prompt Recordings.....	50
8.	Locations of Important IT Materials: .....	51
9.	Restore Plan.....	51
10.	Power .....	51
10.1.	Battery Backup (UPS).....	51
10.2.	Generators – Backup Power.....	52
10.2.1.	Onan 42KW @ JAUNT .....	52
10.2.2.	Briggs and Stratton @ Carter Mountain.....	53
11.	Application & Server: Shutdown & Reboot Procedures .....	53
11.1.	Shutdown Procedures .....	53
11.3.	Restart Procedures.....	53
11.4.	Microsoft Windows 2000/3 – Shutting Down the Server!.....	54
11.5.	Trapeze Software Shut Down and Restart Procedures .....	54
11.6.	MDTAVL Server Application .....	55
11.7.	XGATE Server Application .....	56
12.	Documentation .....	56
12.1.	Acceptable Use of Jaunt's Information Systems Policy .....	56
12.2.	Web Site Privacy Statement .....	59
12.2.1.	"Customer Identifiable" Information.....	59
12.2.2.	JAUNT Online Privacy Policy.....	59
12.2.3.	JAUNT Protects Online "Customer Identifiable" Information as follows:.....	59
12.3.	IP Address Schemes .....	59
12.3.1.	Internal IP's.....	60
12.3.2.	External IP's.....	61
12.4.	Jaunt Phone Lines.....	62

13.	System Disaster Recovery and Preparation.....	62
13.1.	Setting Out to Recover a System: .....	63
13.2.	Emergency Repair Disk/Automated Recovery System.....	63
13.3.	Creating Setup Boot Disks.....	63
13.4.	Starting a System In Safe Mode .....	64
13.5.	Using The ER Disk To Recover a System .....	65
13.6.	Working With the Recovery Console .....	65
13.7.	Installing the Recovery Console as a Startup Option.....	66
13.8.	Starting the Recovery Console .....	66
15.9	Recovery Console Commands .....	66
15.10.	Deleting the Recovery Console .....	68

## 1. JAUNT Network & Mobile Data Configuration Diagrams



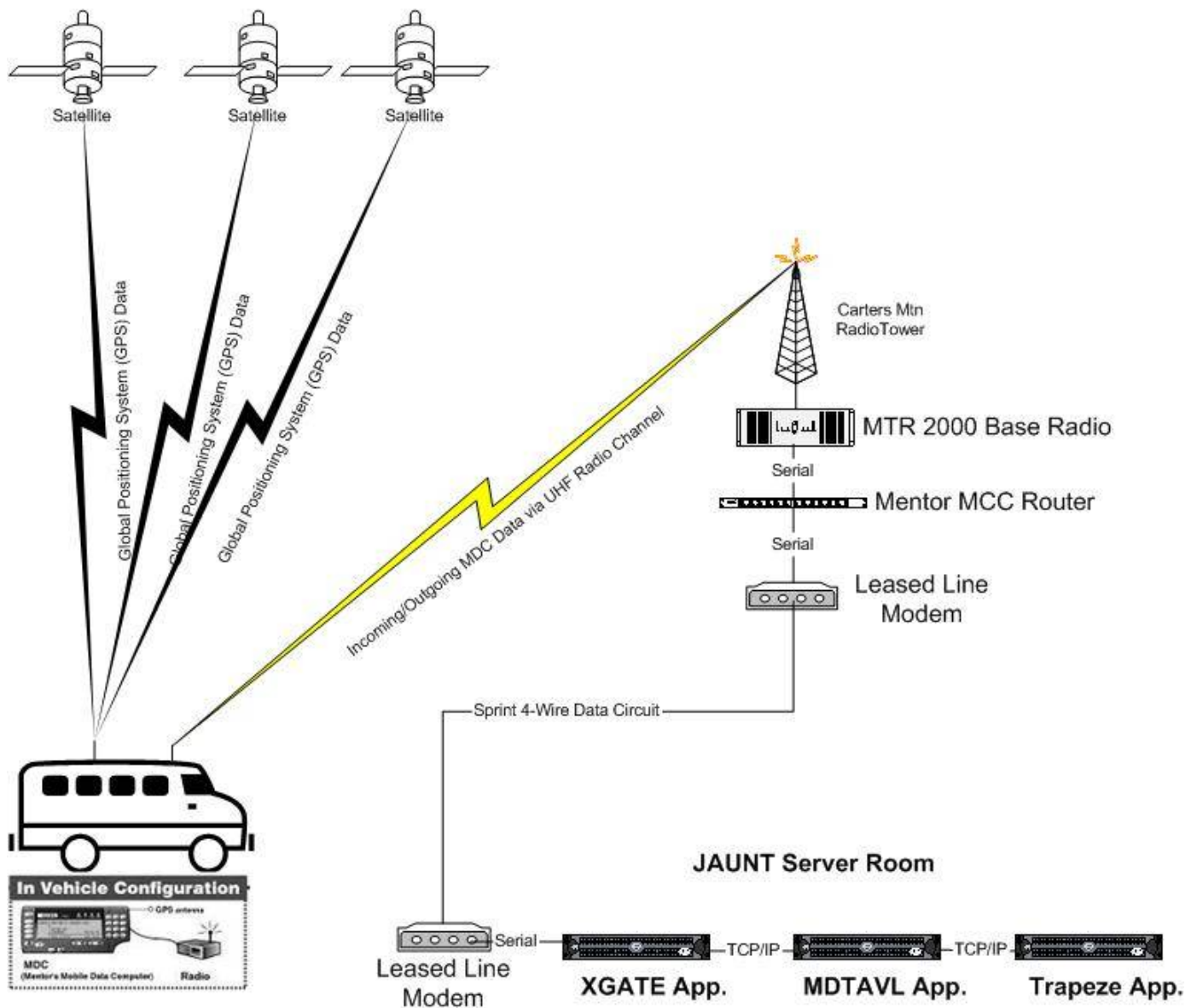
Not in Use

By Kevan Danker



3 Spare 10/100 3Com Switches

# JAUNT MOBILE DATA LAYOUT



Kevan Danker

Mobile Data Configuration.vsd

11/26/2003

## 2. Important Contact Information

### **JAUNT Network Passwords & Other Critical Information:**

<b>Kevan Danker</b> Assistant Director 696 Valley View Rd. Ruckersville, VA 22968 H 434-990-8329 C 434-996-6358	<b>Donna Shauneseay</b> Exec. Director 1003 Birdwood Rd. C'ville, VA 22903 H 434-296-4777 C 434-996-0392	<b>Debbie Taylor</b> Operation Mgr. 97 Riverside Dr. Schuyler, VA 22969 H 434-831-2566 C 434-996-3366	<b>Backup Tapes:</b> Kevan Danker
--	---	--	--------------------------------------

**DELL PC and Server Maintenance** Gold Support PC's 866-876-3355, 2650 Silver Sup 866-410-3355 Gov't Support. 800-234-1490 Write down the DELL Service Tag# before calling.

### **Entre Computer Center – Local Network, PC & Printer Maintenance (no contract):**

For any network, printer, pc problems when IT staff are not available. 434-971-8700 Main line w/instructions for after hour's service. 434-961-2771-Priority service 296-8538-lrv Cox (owner) Home

**Advanced Networking Consultants for Exchange, SQL or advanced Network problems – VASI** (State Contract, 4 Hr.) 800-685-8435, Bell Tech.logix (540-574-4000) or ISIS (804-762-4200) Richmond, (No Contract)

**Great Plains/Dynamics Consulting: Skyline IS, Inc.,** Henry Hickman 434-296-8800

**CISCO Hardware & OS Support PIX 515 & IOS** 800-553-2447 Contract #1385149 #20-P1-577228

**Trapeze Software (TRAPSOFT, TRAPDB, MDTAVL, PASS & IVR, MON, COM):** [cc@trapezesoftware.com](mailto:cc@trapezesoftware.com)  
Customer Care - (877) 411-8727 (8am to 8pm) Webex Sessions – <http://trapezesoftware.webex.com>

**Clear Communications – Two-Way Radios, Tower and 2<sup>nd</sup> Tier MDC Troubleshooting** 434-971-8139

**AVAIL Technologies** (If Trapeze, Mentor or Clear is not available or for MDC's) (814) 234-3394 x-22 (Mon-Fr 8 am to 5 pm), locate operator if Dave is unavailable. [support@availtec.com](mailto:support@availtec.com)

**Mentor Engineering Software & Hardware (MDC, XGATE, MCC)** 403-777-3760, x-3 or [service@mentoreng.com](mailto:service@mentoreng.com)

**3COM Hardware (Switches) Lifetime Warranty** – Demand that replacement be sent before defective switch is returned to them. 800-876-3266

**Seacom** – In-house support for phones and PBX system and computer cabling. 5 yr warranty till 4/2009 817-0252 - Charlottesville

**Intelos – Local Phone Support** 800-323-0457

**Sprint – Long Distance, Local and Leased Line to Radio Tower** 800-795-1004 – Repair, 877-677-7596 - Status Ctr. Long Distance for all JAUNT phone lines and local 434-296-0730 and -1391 and 296-8861

**BNSI - Broadband Network Services Inc – Internet (ISP), T1, CISCO CSU/DSU Router** 434-817-7300

**Cabell Insurance – JAUNT Insurance Agent** 434-977-5313 – Don Thornhill or Lisa Blake, fax (434) 977-3954

**Fidelity Engineering** – Generators maintenance repair and Svc. Agreement for both generators. 800-787-6000

**Lakeside Electric** – Electricians and non-contract generator repair 434-975-3005 or 540-967-3000 or 3057

**Logitree – IVR phone system and servers** (301) 220-3520 x124 or ask for Brent Chism, Mike Gager, or Operator

**Security/Alarms** – Mechums River Security 434-975-0316, emergencies 972-1013



## 3. Equipment Maintenance

All IT equipment will be maintained to ensure maximum up-time and useful life and minimal unexpected maintenance.

### 3.1. Servers

3.1.1. All Servers are scheduled to have maintenance performed weekly and monthly by IT staff via a prescribed list of tasks

### 3.2. PC's

- 3.2.1. Each server and PC desktop is automatically password locked (15 mins) when not in use, requiring a domain username and password to access the servers.
- 3.2.2. All PC's are required to have Virus prevention software, Anti-Spyware software as well as any additional safety measures based on individual PC needs. Updating of virus/spyware definitions and database engines shall be automatic and monitored for performance.
- 3.2.3. Monthly PC maintenance shall be provided to all PC's ensuring; all automated services are working properly, all software and hardware updates are current, no excessive local file storage, optimal system speed, etc.

### 3.3. Other Equipment

3.3.1. All other equipment, i.e., generators, copy machines, etc. will be maintained based on the manufacturer's recommendations and any service agreements.

## 4. Software Maintenance

### 4.1. Trapeze

4.1.1. **Data Archiving** – The data archiving process involves creating a SQL data dump, saving the file and then deleting all the tables from the past for a specified date range.

- All users must be off all applications (unless you done month at a time)
- Ensure a data dump is performed directly before the Archiving process
- On the SQL server (not through PC Anywhere or Remote Desktop) run SQL Query Analyzer.
- File/Open T:\Queries\ArchiveDelete.SQL
- Fill in the start and end dates for each query (MAKE SURE YOU PUT THE PROPER DATES IN THE CORRECT LOCATION!!!)
- Each Query must be run separately in order from top to bottom.

- Deleting Tracker Action Logs every three months since that process takes significantly longer than the others

#### **4.1.2. Database Rebuild** – This process cleans up the database and can decrease the size by up to half.

- Contact Trapeze to schedule time after hours (preferably on Friday eve or Saturday) for them to WebEx in and perform the operation.
- Completed 8/4/2005 and next day's schedule was messed up afterwards, though all trips appeared to be there.
- Make sure schedules for next three days are saved as Word/Excel files
- Complete a data dump with Verification directly before the Rebuild – ensure no one modifies the database during or after dump
- Complete

#### **4.2. Great Plains**

## **5. Security**

JAUNT faces numerous challenges securing its various information systems including its data.

- Identify the need to protect information.  
JAUNT sustains an ever growing compilation of electronic data from financial information to operational data. Accessing and storing this information is critical to the viability of the company.
- Define authorization levels for administrators and users.  
Authorization for all data has been analyzed and is tested to ensure those individuals needing the information have access and those who do not, are blocked.
- Define and Detect Security Threats Internally and Externally  
As the number of types of security threats increase, staff incorporates new measures to detect all known threats without significantly affecting the information flow across the network.
- Implement a comprehensive monitoring policy.  
On-going security tests are performed to determine if initial security settings are correct as well as to detect any inappropriate changes to security. Measures are add as needed to ensure a comprehensive detection process is utilized.
- Define an IT Policy to handle Security Violations  
JAUNT has created both an in-house and web policy to determine parameters for what staff and web users should and should not be doing. If they cross that line, quick measures will be taken to ensure the overall Safety and Security is maintained at JAUNT.
- Correlate this policy with detected security events.  
Specific security violations are specified when applicable.
- Create and Maintain a Disaster Recovery Plan  
JAUNT's Disaster Recovery Plan includes Information Technology as a critical piece to successfully recovering from a disaster. This plan is updated periodically as changes are made.

## 5.1. Facilities

### 5.1.1. Building

- 5.1.1.1. A GE NX-8 control panel and NX-148E display keypads monitors the safety devices in three zones (New 2 story bldg, Operations and Maintenance) and automatically sends an audible alarm and calls out to appropriate emergency personnel through a 24 hour monitoring service.
- 5.1.1.1.1. Doors & 1<sup>st</sup> floor windows use magnetic contact sensors
- 5.1.1.1.2. Motion sensors are placed in hallways to monitor intruders
- 5.1.1.1.3. Smoke, Smoke/Heat and Heat detectors are placed throughout the building
- 5.1.1.1.4. Only staff requiring before/after hours access are provided with appropriate zone security codes
- 5.1.1.1.5. The alarm panel is powered by electricity and has a backup battery to provide 3 hours of backup power.

### 5.1.2. Server Room, etc.

- 5.1.2.1. Neither door into the server room can be unlocked by a master key. The office is locked at all times personnel are not in the room and after office hours. Door sometimes remains unlocked during business hours if frequently used by IT staff.
- 5.1.2.2. Each server and PC desktop is automatically (through Group Policy) password locked when not in use, requiring a domain username and password to access the servers.
- 5.1.2.3. After four incorrect attempts at username and password the computer is locked for 11 minutes.
- 5.1.2.4. The Network Administrator's office including software, hardware, etc. is locked when not in use.
- 5.1.2.5. All Hot-Swappable hard drives (in servers) are locked into their bays, accessible with the appropriate key for all DELL equipment.
- 5.1.2.6. Keys to the server room are limited to only those who absolutely need it.
- 5.1.2.7. A partial spool of CAT5 cable, crimpers and jacks are kept on premise for in-house cable faults as well as provide ad-hoc cabling in temporary facility.

## 5.2. Software & Hardware

### 5.2.1. Active Directory

- 5.2.1.1. We utilize two AD Domain Controller servers to provide redundant Active Directory/Domain services such as DNS, WINS, DHCP, Print Server, Domain Controller, File Server, etc.
- 5.2.1.2. When assigning data access rights to users, group objects are used vs. user names to decrease long term cluttered rights assignments and to help with ensuring outgoing employees do not have any access they shouldn't, due to inadvertent additional user right.

- 5.2.1.3. The Assistant Director periodically peruses through the various sections of AD and cleans up stale resources, searches for and eliminates duplicated entries, breaks out complex GPO's into more manageable objects, etc.

## 5.2.2. Users

- 5.2.2.1. Domain Administrator Account renamed and relabeled.
- 5.2.2.2. Administrator Account then created with Guest rights & very complex password to create a
- 5.2.2.3. Guest Account renamed and disabled.
- 5.2.2.4. Domain Admin account password changed periodically
- 5.2.2.5. Contractors requiring access to Network are given username/password which expires upon day leaving.
- 5.2.2.6. Security of Files and folders is maintained using AD Groups, eliminating difficult-to-manage stray user names.
- 5.2.2.7. Weekly listing of folder permissions is provided to Assistant Director for reviewing accuracy and indication of more effective changes to be made.

## 5.2.3. Exchange Email

- 5.2.3.1. MS Intelligent Message Filtering is utilized on all incoming email to thwart a majority of spam and related unwanted/intrusive email before individuals receive them.
- 5.2.3.2. Outlook's junk email filter and McAfee PC scanner scan all incoming email.
- 5.2.3.3. The Exchange 2003 server, COMM is virus protected by McAfee VirusScan Enterprise (server) and McAfee Groupshield (Exchange)
- 5.2.3.4. COMM is also protected by McAfee Outbreak Manager for any possible outbreaks due to malicious code.

## 5.2.4. Servers & PC's

- 5.2.4.1. Each server is automatically password locked when not in use, requiring a domain username and password to access the servers. IT staff manually lock-down the servers when leaving the room.
- 5.2.4.2. All Servers are required to have Virus prevention software, though active patrolling may be disabled based on individual application requirements. Updating of virus definitions and database engines shall be automatic and monitored for performance.
- 5.2.4.3. Each server and PC desktop is automatically password locked (15 mins) when not in use, requiring a domain username and password to access the servers.
- 5.2.4.4. Monthly PC maintenance is provided to all PC's ensuring; all automated services are working properly, all software and hardware updates are current, no excessive local file storage, optimal system speed, no apparent malware, etc. are present.
- 5.2.4.5. Most all (IVR1&2 utilize RAID 1) Servers utilize SCSI RAID 5 creating a stable and redundant hardware solution allowing one hard drive to fail without data loss nor does the networked information stop flowing, until a new/repaired hard drive replaces the damaged one. With that replacement the system rebuilds all the data on the drive while maintaining services to all users. "Management" utilizes RAID 1 for the OS and RAID 5 for the data storage.
- 5.2.4.6. Servers include redundant fans and power supplies ensuring maximum system uptime.

- 5.2.4.7.** Microsoft Windows Software Update Services
- 5.2.4.7.1. Used to maintain current security, patches and other updates on all Windows machines via Group policy object.
  - 5.2.4.7.2. Centrally managed from one console including single approval of all updates by Assistant Director.
  - 5.2.4.7.3. PC's, laptops and servers (separate GPO) automatically search for any applicable updates once per day at 11 am. PC's and laptops automatically download and install all approved updates and then warn user if reboot is necessary. Servers download and install only after IT Administrator allows it.

## **5.2.5. Desktop Computer Policy**

- 5.2.5.1.** Group Policies & Procedures are currently in use;
- 5.2.5.1.1. Passwords must be 6 characters, include at least one number and cannot be a previous password.
  - 5.2.5.1.2. Passwords must remain for a minimum of 1 day, after 5 incorrect logons, user locked out for 11 minutes.
  - 5.2.5.1.3. Screensaver is automatic with password lockout protection, set to 15 minutes
  - 5.2.5.1.4. "Restricted Users" group used for high risk Users & Computers – **Separate GPO**
  - 5.2.5.1.5. CD Autoplay turned off
  - 5.2.5.1.6. Registry "RunOnce" turned off
  - 5.2.5.1.7. IE settings locked down
    - 5.2.5.1.7.1. Media Player, MSNBC, shockwave disabled
    - 5.2.5.1.7.2. Disabled "Run" menu & Control Panel, command prompt, registry editor
    - 5.2.5.1.7.3. Removed My Documents
    - 5.2.5.1.7.4. Don't save settings on Exit, Auto load COM components if missing
    - 5.2.5.1.7.5. All PC's are required to have Virus prevention software, Anti-Spyware software as well as any additional safety measures based on individual PC needs. Updating of virus/spyware definitions and database engines shall be automatic and monitored for performance.

## **5.2.6. Router/Firewall**

- 5.2.6.1.** The Cisco PIX Firewall/router eliminates the use of any ports and protocols not in use. This three NIC router also maintains a separate DMZ for our web server, separating all web traffic from our internal network.
- 5.2.6.2.** The unit uses one password to enter the device, then a second password to make any configuration changes. Both passwords and management is limited to the Assistant Director's use.

## **5.2.7. Users' Data**

- 5.2.7.1.** Users are trained to save all JAUNT data to network drive Q: (\\root\data\$) which is backed up nightly and verified for viruses, etc.
- 5.2.7.2.** Non-JAUNT data (personal information – i.e., resume, personal letters, etc.) are stored on the P: drive (\\root\users\$) which provides personal secure space for each employee. The data is backed up nightly and monitored for viruses, etc.
- 5.2.7.3.** The hard drive space on the PC's is not backed up though it is monitored for viruses and malware. Any data saved on the local hard drives are not managed nor can be recovered.

- 5.2.7.4.** PC's and Servers utilize NTFS file systems for maximum security and stability for all data storage
- 5.2.7.5.** Yearly analysis of location of highly critical or sensitive data is performed.
- 5.2.7.6.** All PC's and laptops are loaded with McAfee Virus Scan, Microsoft AntiSpyware software and monitored via IT staff management software.

## **5.3. Audits**

IT staff audits security using the following methods:

- 5.3.1.** Perform external security barrages to locate holes coming into the network. Typically these tests are done with free on-line tests that security software/hardware manufactures offer to indicate why you need their products. Private out-sourced Security tests are planned for FY 05/06.
- 5.3.2.** Weekly staff logs onto network as two random users to determine level of access to folders and files
- 5.3.3.** Staff reviews periodically Firewall logs to find abnormalities or trends.
- 5.3.4.** Daily, staff reviews all server hard drive free space looking for abnormalities
- 5.3.5.** Yearly staff determines highest level sensitive data locations and verifies security parameters and verifies those locations are on the weekly user test described above
- 5.3.6.** Monthly, staff performs maintenance on all users PC's looking for abnormalities, verifying appropriate software is operational and systems are not affected,
- 5.3.7.** Microsoft's Software Update Services are used to ensure all critical MS patches are tested then applied in a timely manner to all systems.

## **5.4. Intellectual Property**

- 5.4.1.** All software purchased for JAUNT is added to the inventory list including software security codes, # of licenses etc.
- 5.4.2.** All software is maintained in one of three locations, Assistant Director's office (locked when not in use), Technology Assistant's office and the Server room. No client software is kept locally with the clients.
- 5.4.3.** Drives, folders, files and shares are designed to only provide access to those requiring it by utilizing NTFS file security and a parent/child design.
- 5.4.4.** When users leave the organization, their username is locked out immediately, and a new username is created, not renamed when a replacement is hired, in order to clean any oddities created with the old user.
- 5.4.5.** JAUNT's VPN connection is secured by a 3DES encryption from CISCO and requires a separate logon name and password. Once connected to VPN, NTFS authentication is required for network access.
- 5.4.6.** Users' passwords are automatically forced to change every 60 days, require at least 6 characters and one number and can not be used again for the next six changes.
- 5.4.7.** Default users are not given access to load any programs on PC's without assistance from IT staff.

## **5.5. Clean Up Policy**

### **5.5.1. Employees Leaving the Organization**

- 5.5.1.1. Before they leave:** 1. Ask them to clean out all personal email and archive any useful business Outlook data for next user. 2. Ask them to move all data off any local drives to network folder, 3. Request they turn in any sensitive information printed on paper, 4. Ask them to notify any email recipients of their email change. 5. Ask them to organize their company data for future user's easy access.
- 5.5.1.2. When they leave:** 1. Disable Active Directory account, 2. Change password, 3. Force existing user password change if employee had access to them. 4. Disable/Delete user from Trapeze, Great Plains or any other company application separate from Active Directory.
- 5.5.1.3. When I.T. Staff Leaves Organization:** 1. Disable AD account as soon as they are gone and change password. 2. Make all users change their password. 3. Change both passwords on CISCO PIX and VPN access password. 4. Change passwords on Web Server (Admin, FTP users, etc.). 5. Review all AD accounts to ensure no old accounts are still active.

## **5.5.2. Equipment Disposal**

All hard drives are reformatted and a fresh DOS or Windows partition is then loaded, and verified. All removable media drives are verified to be empty. If an operating system is included with the PC, the organization has the option of preloading the OS or simply provides the Media for the OS.

# **6. JAUNT Disaster Recovery Information**

## **6.1. Business Continuity Plan**

JAUNT increasingly depends on computer-supported information processing and telecommunications. This dependency will continue to grow with the trend toward centralizing information technology within JAUNT administration and Operations.

The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the Operation. A risk analysis which was conducted identified several systems as belonging to risk Category I, comprising those functions whose loss could cause a major impact to the service within 1 hour. It also categorized a majority of functions as Essential, or Category II - requiring processing support within 3 day(s) of an outage. This risk assessment process will be repeated on a regular basis to ensure that changes to our processing and environment are reflected in recovery planning.

JAUNT administration recognizes the low probability of severe damage to data processing telecommunications or support services capabilities that support our transportation operation. Nevertheless, because of the potential impact to JAUNT and our customers, a plan for reducing the risk of damage from a disaster however unlikely is vital. The Business Continuity Plan is designed to reduce the risk to an acceptable level by ensuring the restoration of Critical processing within 5 hours, and all essential production (Category II processing) within 3 day(s) of the outage.

The Plan identifies the critical functions of JAUNT and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response and that the proper steps will be carried out to permit the timely restoration of services.

This Business Continuity Plan specifies the responsibilities of the Business Continuity Management Team, whose mission is to establish Institute level procedures to ensure the continuity of JAUNT's business functions. In the

event of a disaster affecting any of the functional areas, the Business Continuity Management Team serves as liaison between the functional area(s) affected and other offices providing major services.

**Some of the potential causes of failure include:**

- Hard disk subsystem failure
- Power failure
- Air Conditioning failure
- Systems software failure
- Accidental or malicious use of deletion or modification commands/scripts
- Destructive viruses/malware, etc.
- Natural disasters (fire, flood, earthquake, etc.)
- Human error
- Theft or sabotage

### 6.1.1. Priority of Systems

JAUNT has many systems and if an emergency were to be forthcoming and known, there is a possibility items could be taken off site in preparation for the incident. The following items are prioritized resources in such an event:

- 6.1.1.1. External Tape Backup Units – connected to ROOT, Trapsoft and MDTAVL
- 6.1.1.2. Laptops – any available
- 6.1.1.3. PC's – At least 4, more if possible
- 6.1.1.4. Backup 10/100 Switch
- 6.1.1.5. Patch Cables, cable spool, tools
- 6.1.1.6. ROOT
- 6.1.1.7. TRAPSOFT Server
- 6.1.1.8. TRAPDB Server
- 6.1.1.9. MANAGEMENT
- 6.1.1.10. XGATE Server
- 6.1.1.11. MDTAVL Server
- 6.1.1.12. COMM Server
- 6.1.1.13. JAUNTE

### 6.1.2. Priority - Mission Critical

Network or application outage or destruction that would cause an extreme disruption to the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore, or the restoration process is disruptive to the business or other systems.

**Servers/Applications:**

**ROOT** – Provides AD, WIS, DNS, Print Server, File Server (data files), Backup Server

**TRAPSOFT** – Provides all the Trapeze applications for Reservations, Scheduling and Dispatching

**TRAPDB** – Provides database used for the Trapeze applications, necessary for TRAPSOFT applications to operate.

**XGATE** – The server houses the Dynamics (Payroll, AP, AR, HR) database. Although these processes could be done manually, it would be extremely burdensome especially given additional company strains due to the circumstances. This server also provides MDC data to and from the Tower and vans. Must also have TRAPSOFT and MDTAVL app's running.

**MDTAVL** – Provides the middleware software between the Trapsoft application/database and XGATE server to provide functionality to the Mobile Data Computers (MDC's)



## Other:

**Tape Backup Drives** – Both the dual unit (Trapsoft/mdtavl) and single unit (ROOT) would be very beneficial for restoring data from any of the backup tapes since their formatting is specific to the unit and it would most likely be difficult and time consuming to find drives with the same formatting.

**ESI PBX** – Our phone's are the critical communication tool between JAUNT and all our customers. During an outage, passengers would not be able to call in to schedule or change any trips and we would not be able to warn any passengers of any scheduling changes. Our initial phone message all callers hear includes important messages in times of service delays and outages.

### 6.1.2.1. Priority - Important

Network or application outage or destruction that would cause a moderate disruption to the business, cause minor legal or financial ramifications, or provide problems with access to other systems. The targeted system or data requires a moderate effort to restore, or the restoration process is disruptive to the system.

#### Servers/Applications:

**COMM** – Email is an important communication tool though business will proceed without it.

**MDTAVL** – This provides the link between TRAPSOFT and XGATE for routing MDC messages. All 3 server app's have to be running for this to work.

**JAUNTE** – Web server for communicating status and plans with "outside world" during a crisis.

## Other:

**Printer(s)** – Most importantly for printing driver manifests, as well as notices, letters, etc.

**Fax Machine** – To send and receive faxes from other agencies, emergency command stations, etc.

### 6.1.2.2. Priority - Negligible

Network or application outage or destruction that would cause a minor disruption to the business. The targeted systems or network can be easily restored.

#### Servers/Applications:

**MANAGEMENT** – Provides AD, DNS, WINS and some network management tools. This acts as a backup "domain controller" for network resiliency.

**IVR1 & IVR2** – Used for passengers to call and get information about their trips during/after hours. Since this service is only utilized by a very small percentage of our passengers it does not provide a significant loss.

### 6.1.3. Scenarios

#### 6.1.4.Disabled/Inoperable Servers

**6.1.4.1.** Entre Computers and VASI offer replacement servers in case one or more JAUNT servers were to become inoperable for an extended period of time. Both organizations have agreed to providing that service if needed without a contract.

**6.1.4.2.** VASI or Entre could provide restore functionality if needed for JAUNT's DLT backup tapes if no backup hardware is available.

**6.1.4.3.** Redundant hardware including additional hard drive, RAID 5, SCSI, redundant fans, etc. will provide continued service until single unit is replaced.

- 6.1.4.4. When a server goes down, alternate servers will be used whenever possible to provide services for the downed server, i.e., print, WINS, logon, etc.
- 6.1.4.5. Extended warranties and replacement plans have been purchased with hardware whenever possible to provide fast replacement parts and complete replacement units.
- 6.1.5. Inoperable Networked Printers**
  - 6.1.5.1. Multiple networked printers provide redundant resources for printing business critical information during a single or dual printer outage.
  - 6.1.5.2. Several mid range laser printers are connected by wire to PC's. These would provide a backup to any network printing outage.
- 6.1.6. Internal access to network is unavailable**
  - 6.1.6.1. A VPN connection into the JAUNT network is utilized from the Customer Relations office and home of the Assistant Director. Both locations utilize a moveable laptop computer. That connection could provide limited outside access to the JAUNT network data and applications if needed.
  - 6.1.6.2. If internal infrastructure is inoperable the Assistant Director or IT staff person can build any length of CAT5 cable to directly connect any PC
  - 6.1.6.3. Two Spare 10 base hubs and one spare 100 Base hub provide backup for inoperable switches.
- 6.1.7. External Network Outages**
  - 6.1.7.1. BNSI (T-1 & ISP) utilizes two different Internet backbone carriers providing redundant access in case one has a failure.
  - 6.1.7.2. BNSI provides a maximum 24 hour repair if T-1 connection goes down.
  - 6.1.7.3. Backup for the BNSI owned DSU/CSU router would come from BNSI.
  - 6.1.7.4. BNSI provides a modem based Internet connection via phone line - used for longer term outage.
- 6.1.8. Telephone Outages**
  - 6.1.8.1. One analog phone line separate from the main lines provides a redundant POTS line that utilizes separate connectivity through a separate provider (Sprint).
  - 6.1.8.2. JAUNT Cell phones will be deployed.
  - 6.1.8.3. A backup copy of the ESI programming is saved on J312 – Kevan's computer C:\Program Files\Esi-Tools\Esi-Access\Sites\Jaunt.
- 6.1.9. Power Outages**
  - 6.1.9.1. A 45KW generator with an automatic switch provides auxiliary power to specific circuits throughout entire building including the maintenance garage. Heaters for the Admin offices are also powered.
  - 6.1.9.2. All servers are backed up by battery backup's providing short term continuous power until the generator switches power.
- 6.1.10. Carter's Mountain Two Way Radio Tower Facilities**
  - 6.1.10.1. Power Failure - An Uninterruptible Power Supply with surge suppression provides clean power to the data radio and associated equipment during short power outages.
  - 6.1.10.2. Equipment Failure - Spare Equipment for Tower location, located at JAUNT office – Data Radio base station, Mentor MCC router and wiring, Leased line modem
  - 6.1.10.3. Clear Communications provides service for all facilities at tower.
  - 6.1.10.4. Assistant Director and IT staff have appropriate keys and codes to access the tower facilities.
- 6.1.11. On-Board Vehicle Mobile Data Computer (MDC) Outages**
  - 6.1.11.1. Several spare MDC's located in Maintenance garage
  - 6.1.11.2. Spare programming PCMCIA cards located in Assistant Director's office.
  - 6.1.11.3. Maintenance staff, IT staff and Assistant Director can troubleshoot and swap out MDC.
  - 6.1.11.4. Clear Communications will troubleshoot after staff.
- 6.1.12. Recovery Operations**
  - 6.1.12.1. The quickest methods listed above will be used based on priority of problem and safest opportunities.
- 6.1.13. Salvaging Operations**
  - 6.1.13.1. Salvage Team determine which equipment and furniture can be salvaged. Photograph all damaged areas as soon as possible for potential insurance claims.

- 6.1.13.2. Salvage Team Important \*\* Prior to performing any salvage operation contact Insurance Team to coordinate with possible insurance claims requirements and appraisals.
- 6.1.13.3. Have the Physical Plant Supervisor and staff start salvaging any furniture and equipment.
- 6.1.13.4. Based upon advice from Insurance Team and customer engineering, contact computer hardware refurbishers regarding reconditioning of damaged equipment
- 6.1.13.5. Team Leader Meet with the Business Continuity Management Team Coordinator to provide status on salvage operations.

#### 6.1.14. Testing

Testing the Business Continuity Plan is an essential element of preparedness. Partial tests of individual components and recovery plan will be carried out on a regular basis. A comprehensive exercise of our continuity capabilities and support by our designated recovery facilities will be performed on an annual basis. Proper insurance levels and types are reviewed every year to ensure an adequate recovery.

## 6.2. Backup Operations & Procedures

Backups are a last ditch response to recovering lost data. JAUNT backs data up to DLT tapes from ROOT, MDTAVL and TRAPSOFT and DAT tapes on Management and the web servers every evening, rotating the tapes before close of business every day. MANAGEMENT is backed up to itself with a DAT72 tape from its own drive its tape is changed manually also by the end of the working business day. EJAUNT is routinely backed up to itself and then to an external hard drive or DVD.

**Nightly Manifest Backups** - A Word document is created (Trapeze report export) every night containing the Manifests for the next day. Those are stored at Q:\EVERYONE\Backups.

JAUNT uses Veritas Backup Exec for Windows 2000 vs. 10d on all DLT Backup servers.

**Tape Storage** – All “Live” tapes are stored in the safe on the 2<sup>nd</sup> floor. Extra tapes are stored in the Server room.

**Tape Labels** – Mon 1 and 2, Tue 1 and 2, Wed 1 and 2, Thur 1, 2 and 3; Weekend 1 and 2; Month 1, 2 and 3. Mon, Tue, Wed and Weekend tapes are differential tapes and Thursday and Month tapes are full backup tapes. Weekend tapes are inserted on Friday and removed on Monday. The corresponding backup device (server) name is included on the tape label.

The Tape rotation is based on the GFS backup methodology. Generally, All backups are differential backups with the exception of Thursdays. Thursday backups are FULL backups. The last full backup of the month is referred to as a Monthly backup. In order to maintain 3 months worth of data there are 3 monthly tapes (Month #1, #2, #3). Month tapes will be rotated and one is located off site at the IT Assistants home for three months.

The Thursday Full backups are referred to as Weekly FULL backups and are on a 3 week cycle. Each weeks Thursday Full Backup tape is labeled with the week number (i.e. Week1, Week2, Week3).

The differential tapes are on a two week rotation with each differential backup labeled with the day and either #1 or #2 (i.e. Mon #1, Mon #2). Each day's tapes are inserted on the

day of the backup Mon#1 on Monday, Tues #1 on Tuesday. Friday's, Saturdays and Sundays Tapes are labeled as Weekend with either #1 or #2 and are inserted on Friday.

The backups primarily occur in the late evening starting at approximately 7pm. The rotation schedule is in the Outlook Public Folders/Backup Schedule Calendar. That indicates what tape was inserted on which day for that following nightly backup.

### Backup Priorities

- Backup tapes used in ROOT device are *formatted differently* than the tapes used in the Trapsoft and MDTAVL devices, you CANNOT switch any (including cleaning) tapes between the units.
- **All** network resources (data) should be broken down into backup jobs (portions of work). Those individual jobs should;
  - not take an excessive amount of time to backup,
  - include data located on the same server,
  - separate Server services (SQL, Exchange, MSDE, etc) from other data whenever appropriate.
  - Include data that is available (not in use) during similar hours of the day.
  - Be spread out amongst all backup devices for even distribution
- For **critical data** (Legal, Personnel, Trips, Financial, Contracts, etc) a separate job should be maintained in order to closely monitor that job.
- If common data from one server will not fit on one tape,
  - Break out the job into jobs that will effectively fit on a tape
  - Run one of the jobs from a backup server with a light data load
- **Prioritize the daily jobs by their schedule**, whenever possible, based on level of importance of the data. Assumption – the first job is most likely to succeed and the last job is most likely to fail.
  - Ensure that all Media is set with no restrictions on Appending or Overwriting, unless a specific issue is being addressed (be careful).
  - Always make the **first** job “**Overwrite.**” This starts the jobs at the beginning of the tape providing maximum space.
  - Always make the **subsequent** jobs “**Append**, and **Terminate** job if no appendable media is available” This will ensure previous jobs are not overwritten from the beginning, and if there is not enough space, the job will end and not overwrite.
- **Replacing Tapes** - *All tapes (Media) must be monitored for Total bytes written, Total mounts, Soft Read Errors, and Hard Read Errors*, comparing the figures to the other tapes and looking for abnormalities and your gut feel. If a tape or tapes have significantly more errors than the typical tapes, throw it away. If a tape is unable to be “Mounted” and it isn't a brand new tape, throw it away, do not try and get it to mount. Chances are it will eventually fail. It's safer to replace a tape rather than take a risk of keeping a tape which will fail when you need it most.
- The **Backup window** for each backup server should not interfere with JAUNT operation.
  - Start time for individual jobs should be after the last person might use the resource.
  - End time should be before the first person needs to use the resource.
  - Set up software to automatically shut down the jobs if they are not finished by the Start time.

- Each Backup Unit should be scheduled for cleaning based on a less than typical period between the cleaning light turning on. Given that when the automatic light turns on any backup jobs are stalled until the unit is cleaned, typically stopping jobs at night.

When taking the tapes out of the backup units, each tape must be marked with that day's date so we can track how old the tape is and we will know which tape has which day's backup on it.

**ROOT** server backs up itself and the Exchange 2003 **Email** server **COMM**.

**MDTAVL** backs up itself and the **XGATE** SQL MSDE server and **MANAGEMENT**, a backup domain Controller. **Trapsoft** backs up itself, and the **Trapdb** SQL server and **MS Great Plains/Dynamics**. The database is also backed up to [\\Management\GreatPlains\\$](#) directory and on the XGATE\ D:\ Drive. The MS IIS 2000 Web server **Ejaunt** is backed up by two DLT tapes using the Windows backup software or using the external hard drive.

**TRAPEZE database backups** – Automatic SQL Db dumps of the single Trapeze database occur every 5 hours during operating hours (10 am, 3pm, and 8 pm) during the week saved in the \\trapdb\d\$\Microsoft SQL Server\MSSQL\BACKUP\mmsmssql1 directory and additional backups and optimizations occur once per week via SQL. The backups and dumps are then backed up to tape as described above. Every weekday the files in the dump directory are moved to the \Data Dumps (3 days running) sub folder. That folder should only hold the previous 3 complete (3 per day) days of dumps and should not be backed up at all (Diff or Full). Each night BE will backup that days data dumps. The manifests for each morning are saved as Word documents the evening before in case of a system failure Q:\EVERYONE\Backups.

**XGATE Application database Backups** – the JAUNT database is [manually exported](#) to file to the \\XGATE\D\$\Backups directory which is then backed up as described above. Directions for exporting the XGATE “JAUNT” database is attached to this document and located in the T:\Documents\MDC PASS MON directory. This data includes past AVL data of the vehicles and the configuration. Given the low level of importance of current data retrieval, backups are completed every three months or at the time of any XGATE software upgrades.

**Microsoft Dynamics (Great Plains)** MSDE databases are located on XGATE server (D:\). The JAUNT MSDE db is dumped into a file and then backed up using XGATE's Veritas Backup Exec., a local scheduled Windows backup, a SQL scheduled Maintenance backup from TRAPDB (JAUNTxdb) and a local script (D:\GPBKUP.bat) using tasks. The script uses busking as the login name so 4changes in password need to be updated in MS Tasks.

**COMM (Exchange 2003)** backups occur nightly Monday through Friday providing access to individual mailboxes.

### 6.2.1. Recovery

#### **Automated System Recovery (Windows 2003 Servers only):**

Idea of ASR:

Automated System recovery is designed as a last resort tool used to recover a system to certain if System Restore fails, and a fresh install of Windows XP or Server 2003 is not an option. ASR backups record the whole system state as it sits at time of backup. It also records the volume and/or partitioning information so when the recovery need to occur you do not have to spend the time to re-setup volume and partition sizes and labels. More importantly it recovers the complete system state (Registry, Installed Programs, and Data) to the point of the ASR backup occurring.

#### Backing up using ASR:

These are the procedures for performing an ASR Backup:

1. Open up the Windows Backup Utility
2. Start the ASR Recovery Wizard
3. Follow the onscreen instructions and select appropriate media to backup too
4. Create the ASR floppy prompted by the wizard (This is not a Boot Disk)
5. When the floppy finishes, the ASR Backup is complete, please store the storage media and ASR floppy disk in a secure location

#### Restoring using ASR:

These are the procedures for performing an ASR Recovery (Please read instructions before performing operation:

1. Insert the Windows Operating System CD (XP/2003) into the CD and boot off the CD
2. In the first stage of the Windows setup it begins loading necessary files to start the setup/recovery/update process. Before it starts it will ask you to press F6 to install RAID or SCSI drivers. If applicable press F6
3. After the F6 prompt on the bottom or you have finished installing the necessary RAID or SCSI drivers you will see a notification on the bottom to press F2 to start the ASR Recovery. Press F2 now
4. Now the ASR Recovery Wizard will begin. Follow the onscreen instructions to complete the recovery process

**Backup Exec Intelligent Disaster Recovery (IDR):** Several servers are protected by BE's IDR option through IDR floppy disks and CD Images located on \\root\netadmin\$\System States. CD images must be burnt to a CD before use. The Tower style DELL PC's have burners.

**System States:** Individual Server System States are located on the aptly named floppy disks and in the [\\root\netadmin\\$\system states](#) folder as well as the individual Servers'.

## 6.2.2. Backup Responsibilities

#### IT Staff or Designee:

- Changes tapes daily based on the Tape Rotation Schedule
- Records date on tape and marks on rotation schedule each day
- Takes yesterday's tapes home to a safe location understanding that heat, extreme cold, and magnets can severely damage the tapes
- Will not sell, destroy, or damage the tapes in any way
- Brings tapes in each day from their house
- Reviews Job logs and quickly responds to any issues.
- Notifies Assistant Director of any possible problems
- Arranges for other staff to take care of procedures when not at work
- Notifies IT Staff if "Cleaning" light is on immediately (backup will not work until tape unit cleaned).
- Prepares Tape Rotation Schedule
- Monitors the backup jobs for success
- Monitors the data available for Restore, ensuring all backed up data is available for restore
- Troubleshoots any backup problems
- Performs any restore jobs when applicable
- Periodically performs targeted (schedule with most important data tested most frequently) data restore to alternate location verifying backed up data.
- Periodically performs System State Backups on all Servers
- Periodically updates ERD/IDR floppies for all Win Servers

### **6.2.3. Recommended Tape Storage**

The 3 month tape should be stored off site at IT staff's home. The daily tapes pulled from the tape unit should be taken offsite to the designee's home. The tapes should be stored offsite for one night before it is brought back to the site and switched for the next tape. There should always be a least two tape sets offsite for each backup unit. Before taking any tapes home, an employee should sign a document stating that he or she is responsible for the tapes. The on-site tapes are stored in a locked fireproof safe on the second floor of new building section to reduce threat of flooding, fire or other similar tape threats. The safe will be locked at all times.

### **6.2.4. Changing the Tape**

To rewind and release the tape, press the Unload button on the tape drive. The Tape in Use light will begin to blink.

Once the tape has finished rewinding, and the Operate Handle light turns green, pull the handle to release the tape.

If the unit does not indicate “Operate Handle” after a few minutes, the unit is either backing up or is “locked” due to an error – The IT staff person or the Asst. Dir. should be notified ASAP. Given a choice between letting a job complete or canceling the job in order to put the new tape in, choose canceling the job unless directed otherwise by the Assistant Director

The current date is then written on the label on the tape being taken out of the unit.

Fully insert the new tape into the drive until you feel a firm stop. Make sure the label is facing outward. If the unit is automatic, you will hear it begin to work, if not, push the handle down to the fully closed position. The Tape in Use light (yellow) blinks as the tape loads.

**NOTE:** Every time you change the tape, look at the Use Cleaning Tape light. If the light is on clean the tape drive before doing a backup. BACKUPS WILL NOT WORK WHILE THE CLEANING LIGHT IS FLASHING!

#### 6.2.5. Cleaning the Tape Unit

1. If the Use Cleaning Tape light is ON (orange), remove the existing backup tape.
2. Fully insert the cleaning tape into the drive until a firm stop is encountered, making sure the label is facing outward. **NOTE** – The ROOT tape drive can use the FUJI cleaning tapes, TRAPDB and MDTAVL can **ONLY USE** the BENCHMARK Cleaning tape.
3. If there is a manual handle, push the handle down to the closed position. The Tape in Use light (yellow) blinks as the tape loads.
4. When the tape is ready to clean, the Tape in Use light (yellow) glows steadily and cleaning begins automatically.
5. When the Use Cleaning Tape light (orange) stops glowing, the cleaning cycle is complete and the unit should display “Operate Handle”.
6. If the Use Cleaning Tape light remains ON (orange), then a cleaning cycle has not been done, and the cleaning tape has expired and must be replaced.
7. Once the cleaning cycle is complete, remove the cleaning tape and insert the next tape for backing up. Verify the cleaning process takes approx. 2 minutes. If it took approx. 25 sec's, the process did not work.

#### 6.2.6. Restoring Data

Restoring data to a server is the responsibility of the IT staff or contracted staff. Only files needed to be restored should be restored, not the entire system unless it is needed. Several attempts to rectify the server problem will occur before a restore is completed.



When restoring System State, your recovery plan should take into account the fact that the age of the backup tape should not exceed the Active Directory Tombstone Lifetime (this is the length of time that deleted objects are maintained in Active Directory before the system permanently removes them; the default is 60 days). If a tape older than the tombstone is restored, the restore APIs will reject all of the data as out of date. Backups must be done on a regular basis.

If you back up data from an NTFS 5 (Windows 2000 NTFS) volume, you should in most cases restore the data to an NTFS 5 volume. If you restore the data to a FAT or Windows NT 4.0 or earlier NTFS volume, you will lose certain file and folder features and you could lose data as well.

### 6.2.7. How to Backup and Restore the Registry

#### How to back up the registry

Before you edit the registry, export the keys in the registry that you plan to edit, or back up the whole registry. If a problem occurs, you can then follow the steps in the [How to restore the registry](#) section of this article to restore the registry to its previous state.

#### How to export registry keys

You can follow these steps to export a registry key before you edit it:

**NOTE:** Do not follow these steps to export a whole registry hive (for example, HKEY\_CURRENT\_USER). If you must back up whole registry hives, back up the whole registry instead.

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **regedt32**, and then click **OK**.
3. Locate and then click the key that contains the values that you want to edit.
4. On the **Registry** menu, click **Save Key**.
5. In the **Save in** box, select a location in which to save the .reg file, type a file name in the **File name** box, and then click **Save**.

#### How to back up the whole registry

To back up the whole registry, use the Backup utility to create an Emergency Repair Disk (ERD), or back up the System State (which includes the registry, the COM+ Class Registration database, and your boot files). For additional information about using the Backup utility to create an ERD, click the following article number to view the article in the Microsoft Knowledge Base:

[231777](#) How to create an emergency repair disk in Windows 2000

For additional information about using the Backup utility to back up the system state, click the following article number to view the article in the Microsoft Knowledge Base:

[240363](#) How to use the Backup program to back up and restore the system state in Windows 2000

#### How to restore registry keys

To restore registry keys that you exported, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type **regedt32**, and then click **OK**.
3. On the **Registry** menu, click **Restore**.
4. Select the file that you saved, and then click **Open**.
5. Click **Yes** to continue.

#### How to restore the whole registry

To restore the whole registry, restore the System State from a backup. For additional information about using the Backup utility to restore the System State, click the following article number to view the article in the Microsoft Knowledge Base:

[240363](#) How to use the Backup program to back up and restore the system state in Windows 2000

Note that if you use the option to back up the registry when you create an ERD, Backup also creates updated copies of the registry files in the %SystemRoot%\Repair\Regback folder. If you cannot start Windows 2000 after you edit the registry, you can manually replace the registry files in the %SystemRoot%\System32\Config folder with the copies in the %SystemRoot%\Repair\Regback folder by using Recovery Console.

### How to Back Up the System State on a Domain Controller

1. Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
2. Click the **Backup** tab.
3. Click to select the **System State** check box. (All of the components to be backed up are listed in the right pane. You cannot individually select each item.)

**NOTE:** During the system state backup, you must select to back up the Winnt\Sysvol folder. You must also select this option during the restore operation to have a working sysvol after the recovery.

The following information applies only to domain controllers. You can restore member servers the same way, but in normal mode.

If any of the following conditions are not met, the system state is not restored. Backup attempts to restore the system state, but does not succeed.

- The drive letter on which the %SystemRoot% folder is located must be the same as when it was backed up.
- The %SystemRoot% folder must be the same folder as when it was backed up.
- If sysvol or other Active Directory databases were located on another volume, they must exist and have the same drive letters also. The size of the volume does not matter.

[↗ Back to the top](#)

### How to Restore the System State on a Domain Controller

1. To restore the system state on a domain controller, first start the computer in Directory Services Restore Mode. To do so, restart the computer and press the F8 key when you see the **Boot** menu.
2. Choose **Directory Services Restore Mode**.
3. Choose the Windows 2000 installation you are going to recover, and then press ENTER.
4. At the logon prompt, supply the Directory Services Restore mode credentials you supplied during the Dcpromo.exe process.
5. Click **OK** to acknowledge that you are using Safe mode.
6. Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
7. Click the **Restore** tab.
8. Click the appropriate backup media and the system state to restore.

**NOTE:** During the restore operation, the Winnt\Sysvol folder must also be selected to be restored to have a working sysvol after the recovery process. Be sure that the advanced option to restore "junction points and data" is also selected prior to the restore. This ensures that sysvol junction points are re-created.

9. In the **Restore Files to** box, click **Original Location**.

**NOTE:** When you choose to restore a file to an alternative location or to a single file, not all system state data is restored. These options are used mostly for boot files or registry keys.

10. Click **Start Restore**.
11. After the restore process is finished, restart the computer.

## 6.2.8. Returning to the Last Known Good Menu

Changes to the system configuration may keep the system from booting. If you suspect that boot problems are the result of a configuration change, you may be able to correct the problem by returning to a previous configuration. This method is simple and fast, and in some cases will correct boot problems in a Windows computer. There are slightly different procedures for Windows NT and Windows 2000/XP/.NET computers. This section includes procedures for each type of computers.

**Note** Any changes made to the system since the last time the configuration was saved are lost.

#### To return to a previous configuration:

1. Reboot the system.
2. For a Windows NT system, press the spacebar during the startup. The **Hardware Profile/Configuration Recovery** menu appears, which allows you to boot using a previous configuration. For other Windows systems, press <F8> during startup. A menu appears that allows you to diagnose and fix system startup problems. Disaster Preparation of the Windows Computer  
534 *Administrator's Guide*
3. Select one of the following options:
  - **Safe Mode.** This option allows you to diagnose and fix system startup problems. For more information, see your Microsoft documentation.
  - **Last Known Good Configuration.** This option allows you to return to a previous saved configuration.

## Creating an Emergency Repair Disk

When Windows NT or Windows 2000 Server is installed, the installation program prompts you to create an Emergency Repair Disk (ERD). This disk contains system information that can help get the system running in the event of a disaster. It is important to keep the ERD updated whenever system changes are made. The ERD is only useful if it is kept current.

For Windows XP or .NET, Emergency Repair Disk has been replaced with Automated System Recovery (ASR). Whenever a major change is made to the system, make a fresh copy of the ERD before and after the change is made. Major changes include adding, removing, or otherwise modifying hard drives or partitions, file systems, configurations, and so forth. As a general rule, update the ERD before and after the hard drive configuration is changed. The addition of a new component to the server, such as Microsoft Exchange Server or Microsoft SQL Server, and changes from Control Panel, are also situations in which the ERD should be refreshed both before and after the change. Also remember to make a backup of the ERD; always keep an ERD from at least one generation back. When creating a fresh ERD, use a floppy disk that can be reformatted, because RDISK.EXE, the program that creates the ERD, always formats the floppy disk. **Note** The Emergency Repair Disk is a useful and necessary tool; it is NOT a bootable disk. There is not enough space on the disk for the boot files and the repair information files.

Disaster Preparation of the Windows Computer  
536 *Administrator's Guide*

#### To create the ERD for Windows 2000:

**Note** You must not change or delete the `systemroot\repair` folder because the repair process relies on information saved in this folder.

1. Click **Start**, point to **Programs**, and then to **Accessories**.
2. Point to **System Tools**, and then click **Backup**.
3. On the **Tools** menu, click **Create an Emergency Repair Disk**.
4. Insert a disk into the A: drive and follow the instructions.

**Note** The **Also back up the registry to the repair directory** option saves your current registry files in a folder within the `systemroot\repair` folder. This option is beneficial in the event your hard disk fails and you need to recover your system.

## Using Windows' Automated System Recovery and System Restore to Recover a Windows XP or Windows 2003 System

The ASR feature, which replaces the Emergency Repair Disk for Windows XP and Windows 2003, allows you to restore the operating system to a previous state so that you can start Windows XP Professional or Windows 2003 when other recovery methods do not work.

Microsoft recommends using System Restore, which saves only incremental changes, or shadow copies, and lets you start Windows XP Professional in normal or safe mode,

before resorting to ASR. For more information about ASR or System Restore, refer to your Microsoft documentation.

## Creating and Using an Emergency Boot Diskette

**Tip** If the system will not boot, use the Windows installation disks to boot it or use an Emergency boot diskette, which is a quicker way of getting the system up and running. After booting from the Emergency boot diskette, go directly into the existing Windows partition, even if a critical file in the system partition has been deleted or corrupted.

Instructions are provided for creating Emergency boot diskettes on the following types of systems:

- x86 systems (see [“To create an Emergency boot diskette \(x86 version\):”](#) on page 538)

- Mirrored boot partitions (see [“To create an Emergency boot diskette \(Mirrored boot partition\):”](#) on page 539)

Disaster Preparation of the Windows Computer  
538 *Administrator's Guide*

**Note** The boot diskette is NOT generic for every Windows machine. If there is a fairly standard configuration across several machines, however, this disk will work. For example, it will work for all systems that use the same partition and disk controller as their Windows boot partition.

### To create an Emergency boot diskette (x86 version):

1. Format a diskette (the diskette must be formatted under Windows).
2. Copy the following files to the diskette from the root directory of the system partition:

- BOOT.INI
- NTBOOTDD.SYS (if present)
- NTDETECT.COM
- NTLDR

The file NTBOOTDD.SYS is present only if a SCSI controller exists that does not use its BIOS to control the boot process. If NTBOOTDD.SYS is not on the boot partition, it is not needed.

## 6.2.9. Methods for Restoring Replicated Domain Data

There are three different ways to restore replicated data:

- **Non-authoritative restore (default).** A *non-authoritative* restore results in the restored data (which may be out-of-date) becoming synchronized with the data on other domain controllers through replication. That is, data from non-failed domain controllers is replicated to the newly restored domain controller. Most restores are non-authoritative. This type of restore is used to provide a start point (the point of time at which backup was taken) for data replication to minimize the replication traffic on the network—only changed data (rather than the entire directory) is replicated. In the absence of this start point, all data would be replicated from other servers.
- **Authoritative restore.** In contrast, an *authoritative* restore causes the restored domain controller's replicated data to be authoritative in relation to its replication partners. Such a restore is unusual, but, when used, has the effect of rolling back the entire network to the point in time of the backup. This action may be used to restore erroneously deleted information of a replicated set of data.

- **Primary restore.** Use this type of restore when the server you are trying to restore is the only working server of a replicated data set (the Sysvol, for example, is a replicated data set). Typically, perform a primary restore only when all the domain controllers in the domain are lost, and you are trying to rebuild the domain from backup. Select primary restore for the first domain controller and non-authoritative restore for all the other domain controllers.

Table 1 shows which type of restore applies to which type of replicated data:

**Table 1. Use the appropriate restore method for each type of replicated data.**

Type of Replicated Data	Non-Authoritative Restore	Authoritative Restore	Primary Restore
Active Directory	Default	Note 1	Not applicable.
Replicated Data Sets (e.g., Sysvol)	Default	Note 2	Use the 'Advanced restore' option in Ntbackup.
Cluster Database	Default	Note 3	Not applicable.
<p>Note 1: To accomplish this, use the Ntdsutil utility after performing the restore process (where to find Ntdsutil and how to do this procedure are described later in this paper).</p> <p>Note 2: To accomplish this, restore the data to an alternative directory and manually copy the data back to the original directory. The copy will then be the latest source, and it will be propagated to all replicas.</p> <p>Note 3: To accomplish this, use the Clusrest utility (found in the Windows 2000 Server Resource Kit). This will copy the restored quorum data to the quorum disk.</p>			

If you have to perform a restore, several server services require special attention to make them operational. Table 3 lists the services that require additional effort. The subsections that follow the table provide additional information about restoring each service. The final subsection tells you how to verify the successful restoration of distributed services.

**Table 3. How to handle server services when performing a restore**

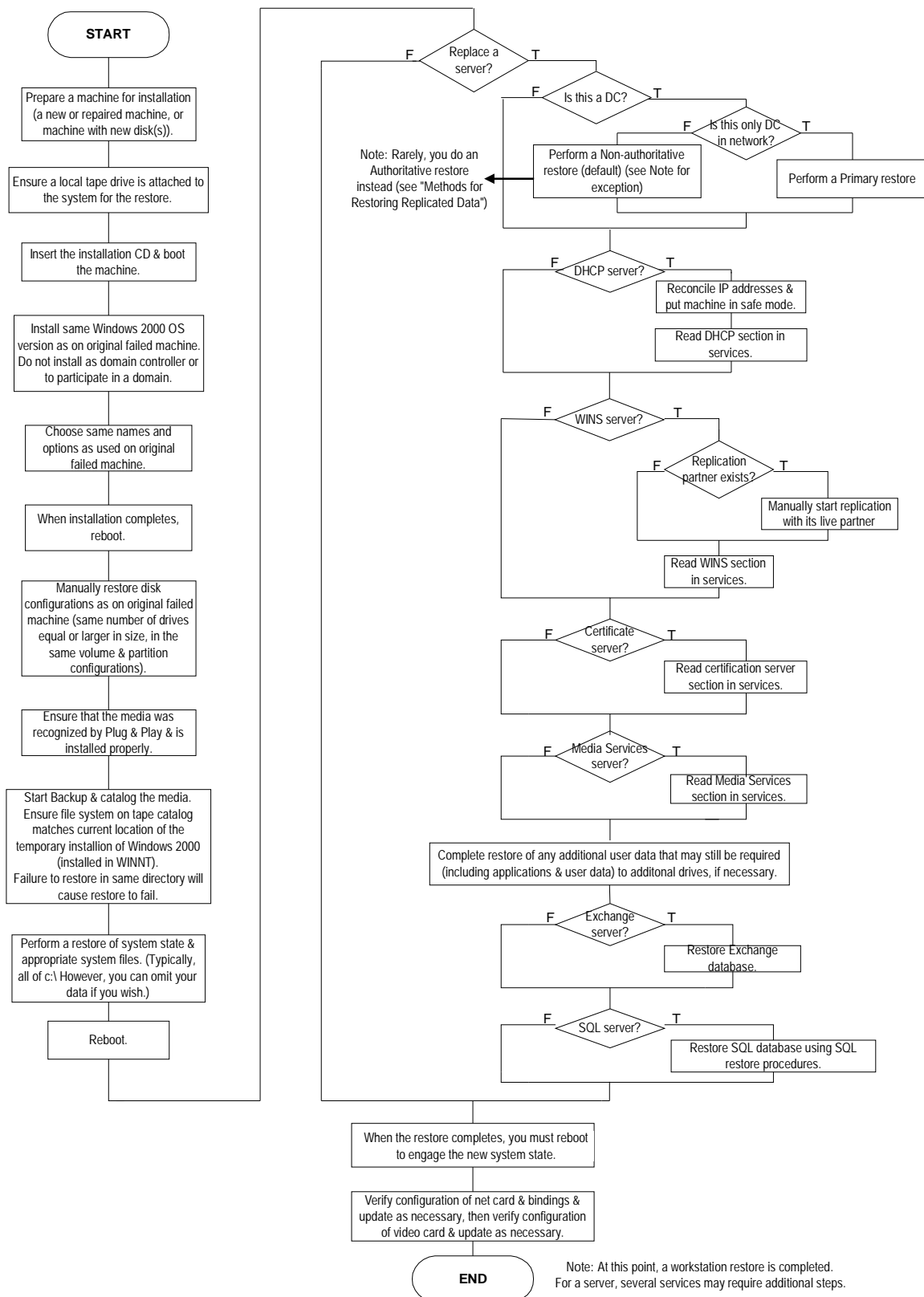
Component	Issue
WINS	The WINS database is restored to the state it was in at the time of the backup. This may not represent the current state. (See WINS subsection below.)
DHCP	DHCP leases are restored to the state at the time of the backup. You must perform several steps to reconcile the state of this database to the current state of the network. (See DHCP subsection below.)
Remote Storage	During a restore operation, the Remote Storage database is recalled from tape media upon restarting the service—but only if the tapes are available. (See Remote Storage subsection below.)
Certificate Services server	After a restore operation, the Certificate Services server may have outstanding certificates that are now unknown. You can revoke and reissue these certificates or leave the old certificates orphaned. (See Certificate Services Server subsection below.)
Windows Media Services server	After a restore operation, you may have to reinstall the Windows Media Services server because the database containing setup information may be lost. (See Windows Media Services Server subsection below.)

Internet Information Services server (IIS)	If you perform a complete restore, no problems with IIS should arise. If you perform a partial restore, you must follow the backup/restore procedures specific to the IIS service. (See IIS subsection below.)
Active Directory	In a network with more than one domain controller, the default restore method (non-authoritative) is generally the preferred method to restore a failed server. Use the authoritative restore process outlined later in this paper <i>only</i> if you want to get the system back to the state at the time the backup was made(which you would want to do in the case when you erroneously deleted Active Directory objects from the database and you would find it difficult to re-create them). (See Active Directory subsection below.)
Sysvol	If the machine being restored is the only domain controller on the network, you must select a primary restore under the advanced restore options in Backup. Otherwise, use the default (non-authoritative) restore. (See Sysvol subsection below.)

## 6.2.10. FLOWCHART FOR SYSTEM RESTORATION

The flowchart in Figure 2 outlines the steps for restoring a system from a state of complete failure to a known point in time. The flowchart outlines the system restore process at a general level. The details of the processes and applications involved are discussed in the following sections.

**Figure 2. Steps to restore a system from a state of complete failure to a known point in time**



## 6.3. XGate 3.1 – Backup Procedure

### Summary

XGate configuration information (channels, units etc.) and logged data are stored in an SQL database. This document describes the procedure for backing up and restoring this database.

### 6.3.1. Creating a Backup of the SQL Database (.XDB File)

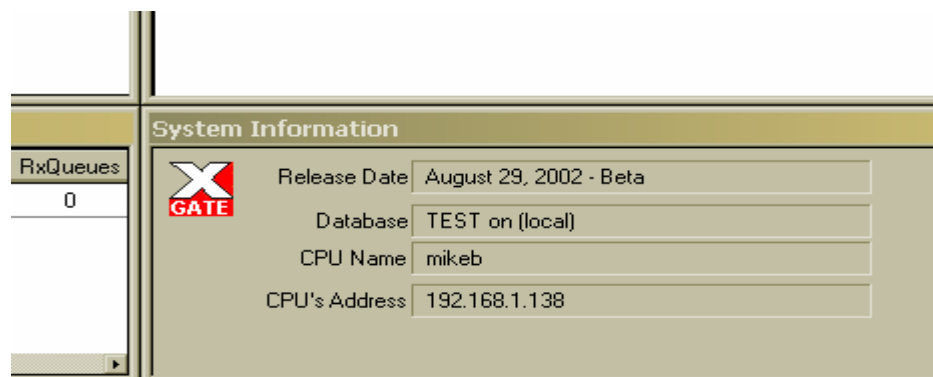
Steps to Export the current SQL database to an .XDB file for backup purposes

Start XGate

Observe the following from the XGate application as demonstrated by the following screenshots:

The SQL Database Name

The SQL Server Name



The “Database” line describes the SQL Database that is running on the SQL Server. For example, in the screen shot above, “Database: TEST on (local)” means the SQL Database: TEST is running on the SQL Server: (local) Use “**JAUNT**”

From the File menu, select Export Database.


A dialog box will appear that indicates the Export Database wizard has been started.

Click “Begin” to continue.



A dialog box will appear. The drop down menu contains a list of all computers on the LAN that are acting as SQL Servers. Select the SQL Server Name you determined in (b) above.

Step 1 of 4



Below is a list of all the active SQL Servers on your network.

Please select the SQL server XGate should use:

SQL Server


< Back

Next >

**6.3.1.1.** Click Next.

A dialog box will appear. The drop down menu contains a list of all available SQL databases on the SQL Server. Select the SQL Database you determined in (b) above (**JAUNT**).

Step 2 of 4



Below is a list of all Databases in the chosen SQL Sever.

Please choose the database to export.

Database

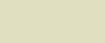
< Back

Next >

**6.3.1.2.** Click Next.

A dialog box will appear asking which logs to export. Select ALL.

Step 3 of 5



Please specify which logs to include in the export

☒ All [.xdb file]

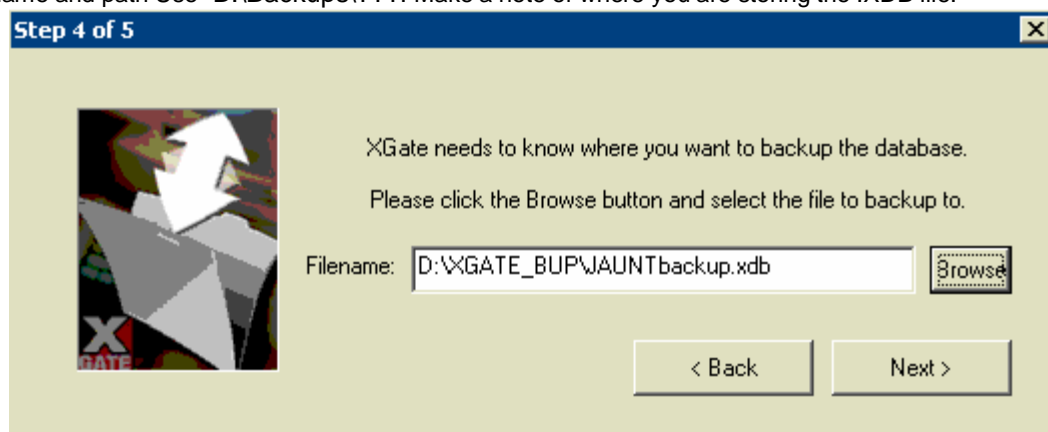
☐ Range\*    Start Date:  Time:   
End Date:  Time:

☐ None\*

\* Exported to .mdb file

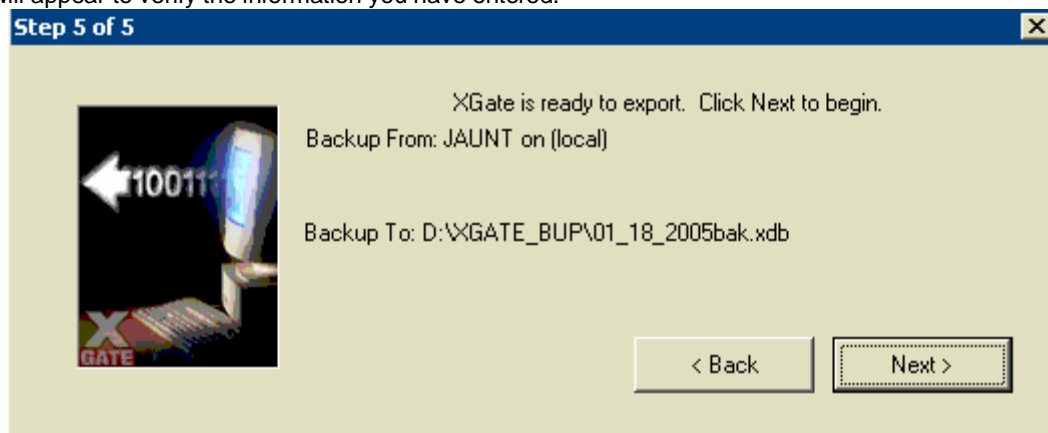
**6.3.1.3.** Click Next

A dialog box will appear asking for the .XDB filename and location you wish to export the SQL Database to. Select Browse and provide a filename and path Use "D:\Backups\???. Make a note of where you are storing the .XDB file.



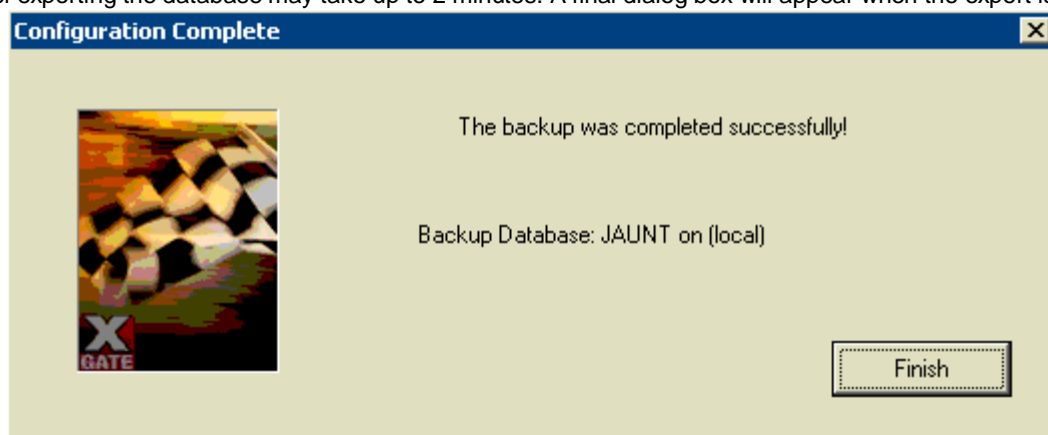
6.3.1.4. Click Next

A dialog box will appear to verify the information you have entered.



6.3.1.5. Click Next.

The process of exporting the database may take up to 2 minutes. A final dialog box will appear when the export is complete.



6.3.1.6. Click Finish.

6.3.1.7.

**NOTE:** It is recommended that the .XDB file you just created be stored on a separate server or backed up on a CD. This will prevent losing the XGate database in case of a hard drive or other computer failure

### 6.3.2. Restoring a SQL Database From an .XDB File

Steps to restore the XGate server using a backup .XDB file.

The steps required to restore the XGate PC are exactly the same as reinstalling XGate with one exception: the backup .XDB file should be selected.

The installation and Initial setup of XGate 3 is described in detail in the XGate 3 manual. When XGate 3 is started for the first time the Initial Setup wizard will start automatically. From the Initial Setup wizard follow these steps

STEP 1: Selecting an SQL Server

Select the SQL Server you wish to use

STEP 2: Choosing a Configuration Database

Select "Import a Configuration Database from an existing file" and click Next

STEP 3: Select the File to Import

Click Browse (D:\XGATE\_BUP\) and select the appropriate backup .XDB file.

Follow the remaining prompts as described in the XGate 3.0 Manual

### 6.3.3. System State Backup

The Xgate system state is backed up weekly by the NT Backup procedure. The file, xgate.bkf, is located on the Xgate server on c:\system state. Veritas backs up this file as part of its normal backup routine.

## 6.4. Backup Exec vs. 9.X – Software Installation Codes

See [\\Management\DS\NetDrive\Data\Senior Staff\EVERYONE\MASTER IT Inventory.xls](#) for latest Installation Codes.

### 6.4.1. Veritas Disaster Recovery Links

**Disaster Recovery shortcut list** - Go to <http://seer.support.veritas.com/docs/261700.htm> for links on backing up and restoring Veritas backups and Windows information.

## 7. Equipment Configurations

## 7.1. Servers

### 7.1.1. MOTHER

This server is a Windows 2003 Server SP1 primary domain controller. This server also shares the primary business files needed for JAUNT associates to access. It also hosts certificate servers, printer sharing, and also servers as a DNS/WINS server.

**Hardware:**

DELL 2850

**With the following services running:** DNS, WINS, DHCP, AD, Print Server, File Server, Certificate Services

**With the following Programs running:** All windows service bound processes listed above.

**Disk Management:**

C:\ is the Operating System Volume

D:\ is the main Data Storage Volume

E:\ is the secondary Data Storage Volume

### 7.1.2. TRAPSOFT

This server hosts our Trapeze application for scheduling and dispatching trips. The program utilizes an active log file that must also be running while the program runs. **TO Shutdown** the software, make sure all users have closed the program from their PC's. Close the SchedServ2 application *then* the SchedServ2 – CDBLOG. To Restart, double click on Schedule Server application (Looks like waiter holding a drink), the log will automatically restart.

Win 2K SP3

**Hardware:**

DELL Poweredge 2650, 2.2 GHz/512K Cache Xeon, 1 GB DDR RAM 200 MHz, Three 18 GB SCSI 15K HD's, Dual on-board NIC's, RAID 5, Dual 500 W Power Supplies

**With the following Services & Programs running:**

PCAnywhere Host, UPS APC Powerchute Plus, Terminal Services, WebEx, Trapeze 4 Client, Trapeze Sched. Server, Backup Exec & Open File Option

**Disk Management:**

### 7.1.3. TRAPDB

This server hosts our SQL Server 2000 Trapeze Database and Microsoft SUS

Win 2K SP3, SQL 2000 (All Trapeze databases)

**Hardware:**

DELL Poweredge 2650, DUAL - 2.2 GHz/512K Cache Xeon, 2 GB DDR RAM 200 MHz, Three 18 GB SCSI 15K HD's, Dual on-board NIC's, RAID 5, Dual 500 W Power Supplies

**With the following Services & Programs running:**

PCAnywhere Host, UPS APC Powerchute Plus, Terminal Services, WebEx, Trapeze 4 Client, Trapeze Sched. Server, Backup Exec & Open File Option

### 7.1.4. MDTAVL

This server hosts our Trapeze Mobile Data Computer application.

MS Win 2K SP3

**Hardware:**

DELL Poweredge 2650, 2.2 GHz/512K Cache Xeon, 1 GB DDR RAM 200 MHz, Three 18 GB SCSI 15K HD's, Dual on-board NIC's, RAID 5, Dual 500 W Power Supplies

**With the following Services & Programs running:**

MDT Server Software (do not log off server, lock the workstation), (software must stay running, do not log off server, lock the workstation) PCAnywhere Host, UPS APC Powerchute Plus, Terminal Services, WebEx, Trapeze 4 Client, MDTAVL Server App., Backup Exec & Open File Option

### 7.1.5. XGATE

This server hosts our XGATE SQL database and application and Great Plains/Dynamics Financial SQL Databases.

**With the following Programs running:**

Xgate 3.0-needs to run at all times, do not log off server, lock the workstation  
PCAnywhere, McAfee Netshield, MS SQL MSDE Server 2000

Win 2K SP3

**Hardware:**

DELL Poweredge 2650, 2.2 GHz/512K Cache Xeon, 1 GB DDR RAM 200 MHz, Three 18 GB SCSI 15K HD's, Dual on-board NIC's, RAID 5, Dual 500 W Power Supplies

**With the following Services & Programs running:**

PCAnywhere Host, UPS APC Powerchute Plus, Terminal Services, WebEx, Trapeze 4 Client, Trapeze Sched. Server, Backup Exec & Open File Option

**Local Admin Account:**

“Administrator” same password as network administrator

### 7.1.6. IVR1

This server hosts our IVR system. Both IVR servers are remotely managed by LogicTree Corp. though Windows updates etc. are updated locally.

**Hardware:**

HP DL380 G3 2.8 GHz Pentium IV, 1 GB RAM, Video – ATI Rage XL PCI, Two NIC's HP NC7781 GB, 3 ½" floppy, SCSI Smart Array 5i, Two HD's HP 36.4 GB 10K RPM Ultra 320 SCSI, RAID 1 + 0, NUANCE software, HP iLO Mgt. Interface Card, VNC software PCAnywhere Host, SQL

### 7.1.7. IVR2

This server hosts our IVR system. Both IVR servers are remotely managed by LogicTree Corp. though Windows updates etc. are updated locally.

**Hardware:**

HP DL380 G3 2.8 GHz Pentium IV, 1 GB RAM, Video – ATI Rage XL PCI, Two NIC's HP NC7781 GB, 3 ½" floppy, SCSI Smart Array 5i, Two HD's HP 36.4 GB 10K RPM Ultra 320 SCSI, RAID 1 + 0, 4 port, 8 line POTS NMS AG2000 card, NUANCE software, HP iLO Mgt. Interface Card, VNC software PCAnywhere Host.

### 7.1.8. COMM

This server hosts Exchange 2003, including Outlook Web Access, Mobile Access.

**Hardware:**

Dell 2850.

### 7.1.9. HVAC

This server hosts our Heating and Air conditioning systems Johnson Controls interface. The system monitors the Water Source Heat Pumps, Water tower, Pumps, Energy Recovery Unit, Make-Up Air Unit, Garage systems, Water temperatures and flow, etc. This also controls the external DVD burner unit.

**Hardware:**

Open Systems PC

### 7.1.10. MANAGEMENT

This server is used as a DNS server, along with being a secondary Domain Controller. It also has some WINS functionality. Windows 2003

**Hardware:**

Dell PE2850, PE2850 3.4GHZ/2MB XEON 800 FSB3.4GHz/2MB Cache Intel Xeon 800MHz-R, 4GB DDR2 400MHz (2X2GB) Dual Ranked DIMMs, Riser ROMB PCI-X PE2850, 4 36GB U320 SCSI 1IN 15K, Floppy, 24X IDE CD-RW/DVD ROM Drive, RAID 5

### 7.1.11. JAUNTE

This is the Windows 2003 Server Web server. It host both the Ridejaunt.org domain namespace but also the CTAV.org domain space. The server is located in the DMZ and access to the server from the internal network is possible however, connection starting from the server to the internal network is prohibited.

**Hardware:**

**With the following services running:**

**With the following programs running:**

**Disk Management:**

## 7.2. PC Configurations

**Printers:**

Networked – (Reservationist Laser, Business Office Laser & Check Printer), local printer if one exists, color printer users connect to HP OfficeJet D155xi – must use CD from KD's office

Radeon 7500, 40 GB EIDE 7200 RPM HD, 3.5" Floppy, PS/2 MS Intellimouse, Intel Gigabit NIC w/alert, 48x EIDE CDROM, Integrated Soundblaster AC97, Internal Chassis speaker, McAfee Virusscan 6.01, NBD P&L Onsite 5 years, gold support

**Network:**

**Protocol:** IP

DHCP for IP and DNS

**PC Name:** "J" then the 3 digit JAUNT inventory # expl. J225

**DELL Optiplex GX260 Small MiniTower PC's**

Same as Small Desktop except: Two 80 GB HD's, 32XDVD-CDRW  
V.92 Modem, Sound Blaster Live 512 Voice Sound

**DELL Optiplex GX260 Small Desktop PC's**

P4 2.26 GHz, 533FSB, 512K Cache, 1 Gb 266 MHz DDR, 17.9" Trinitron, 32 MB ATI

**DELL PC Software:** MS Office Std. or Professional, WinZip, Acrobat Reader, Trapeze, Outlook

**7.3. Firewall, CSU/DSU & Router - CISCO PIX Configuration**

For the latest version of the PIX Configuration settings see R:\Hardware\Cisco\PIX\Configs

**7.4. Phone System - ESI****ESI Phone System: Installer Password – 8822 \*\*Use caution when in Installer Programming\*\* Administrator Password – 1023**

IVX E-Class Gen II system with 3 6x12 port cards and one A12 card. This allows 18 incoming CO lines, 36 digital extensions and 12 analog extensions. Some analog extensions are directly connected to the LogicTree IVR via 2 large biscuit jacks located next to the router.

We currently have 12 phone lines coming into the system 9 of which are in a hunt group. Line 9 is only used only for outgoing calls.

We currently have 3 extra phones in the server room in white boxes marked ESI.

If the system goes down for any reason or there is an indication that it needs to be rebooted, use the switch on the APC ES-500 (located next to the phone switch) to power off the switch and then to turn it back on. It will take approximately 4 to 5 minutes to fully boot. The lights above the amphenol (cable) connectors on the side of the switch will blink in a random fashion, and then only those port cards with active lines in use will glow steadily.

If the need arises to move an extension, the Assistant Director or IT Staff can do it or [call John Hooper](#) at Seacom to do the move; you must be very careful not to short a line (touching the two, disconnects the line) when working with hot wires.

**7.4.1. How to Use**



#### 7.4.1.1. Conference Call

##### Conference Call Setup

1. While on phone with first person
2. Press CONF key (provides tone)
3. Call party to add
4. Press CONF to connect everyone together
5. For additional people - Repeat steps 2 - 4

To connect person on hold:

Press hold key then appropriate LINE # Key

Press flash key if line busy or person not there, you'll be returned to conferees

Press appropriate LINE key to drop an individual

Hang up to disconnect everyone

#### 7.4.2. Programming

Instructions on basic programming can be found in the ESI Administrators Manual located on \\root\netadmin\$\hardware\telephones. There is also a User Guide that describes how to use the basic phone system features.

Any programming needed other than what can be accomplished from the Administrators manual should be done by Seacom, as the Installer has access to system features that can disable the phone system completely.

To Modify System Program

Press "Program" then "Hold"

Enter Passwd

Go to Admin Manual pg. A.3 for shortcuts

To re-record the initial system greeting (MB400-Typically is blank) for special announcements follow the steps here:

From inside JAUNT - Press Program, \*, 400#, 400#. From Outside JAUNT - Call JAUNT, Press \*400, 400, 5

You will be prompted by a menu, follow it to re-record the main greeting. Press "1" quickly after you are done recording to alleviate a pause between MB400 and I D4. Remember, users cannot access the

To test your recording, simply dial Jaunt's main number and listen to the greeting. If you need to re-record the message, follow the above steps. This same greeting is used for day and night messages.

**\*\*Re-record the message back to its normal state after the need for the changed greeting has expired\*\***

Find Deleted Voicemails - Program, Voice Mail, 9

To turn off the Hands Free Speaker (IVR fix for 100, 103, 114 and 117) - Prog, 3, 5 - If someone transfers a call the phone will ring and Speaker will not pick up.

To Re-record the prompts press Prog, Hold, 1023#, 6, 1 then enter the ID#

To turn on Headset functionality, do the following: Press Program, then 3, 3 again, 1, then #, then the Release key. This will enable the headset.

To turn off Headset functionality do the following: Press Program, then 3, 3 again, 0, then #, then the release key. This will disable the headset.

NOTE: Whenever the Headset is enabled, you MUST use the Headset/Answer key located on the bottom left of your gray station keys. Even if you choose to use the handset while Headset is enabled, you MUST use the Headset/Answer key.

To save a voicemail so that the voicemail notification light remains blinking, press 9 twice at the end of the message that will, 'Save as New'.

It is preferable to use Exclusive Hold (by pressing the Hold key for 2 seconds) than a system hold. This will prevent anyone from picking up your call and prevent the Hold key on everyone's phone from blinking.

Remember, try to transfer calls directly to a person instead of intercom-ing them to see if they are there; simply do a blind transfer and hang up.

The ACD reports are back on the phone and you can get them by hooking the laptop up the phone via serial and go through HyperTerminal and choose the phone.xx file saved and then choose receive. Then go into the phone system with the installer password 1024 and choose option 7, then 3( you will have to push # to accept it) and then 1 for current ACD report. Hang up to exit. That will end up as a text file on your PC that you can see what kind of activity the ACD groups have had.

To change the programming for a voice mail box, Program, installer, 3, 3, xxx#, #, #,

### **Recording System Prompts:**

Enter Installer programming. Choose option 6, then option 1. Enter the branch ID you wish to re-record and follow the instructions to record the new prompt. Be aware that as soon as you confirm the recording by using the # key, the recording is saved and active for callers to hear.

### **Recording Virtual/Information Mailbox prompts:**

To Re-record the prompt for Information Mailbox 400, press Program, \*, then enter 400. The password for the mailbox is 400. Follow the instructions to re-record the prompt, save your recording with the # key. For the Reservations and Dispatch Mailboxes, use 300 for Reservations and 301 for Dispatch.

### **Changing an Extensions name:**

Enter Installer programming. Choose option 3, and then option 1. You can enter the persons name by pushing a number key which corresponds to the letter you wish to use. Press the button more than once to scroll though the letters on the key. To select a letter, push the # key. When you are finished spelling a name, push # to accept the change. If you need to start over, press the Hold key to erase the name.

#### **Adding a person to a group:**

Enter Installer programming. Choose option 3, then 3 again. Enter the department group you wish to modify; it can be an ALL group or an ACD group. Press # until you get to the list of extensions. Add the person's extension and press # to accept. Exit programming by pushing the release key.

**\*\*Remember, if you are adding a person to an ACD group, you must also program one of their station keys to be an agent log on/log off key. Do this by choosing a key to use, hold it down to enter programming mode and enter 5XXX, where XXX equals the ACD department group you added the person to.\*\***

#### **Disabling a Mailbox:**

Enter voicemail programming by pushing Program, then 1. Select whichever personal greeting you normally use. When prompted, choose to delete your personal greeting. The system will prompt you that deleting your personal greeting will disable your mailbox, accept this by pressing the # key. The mailbox will now be disabled. Calls will be routed by the Call Forward/Busy/No Answer programming.

#### **Enabling Headset Functionality:**

Press Program, 3, 3 then choose 1 to enable the feature and 0 to disable it. Remember, you must then program a station key to be your headset answer/release key by using the code 564 on the chosen key. Simply plug the headset into the jack on the back of the phone to connect.

#### **Virtual Mailbox Key**

Provides voice mailbox access for any user, other than their extension#. Choose a station key to program, then push the Voice Mail key and then enter the number of the mailbox you wish to monitor. The button will blink when there is a message in the box, push the button to enter and retrieve the message.

#### **Adding a Speed Dial Number to the System ESI-DEX**

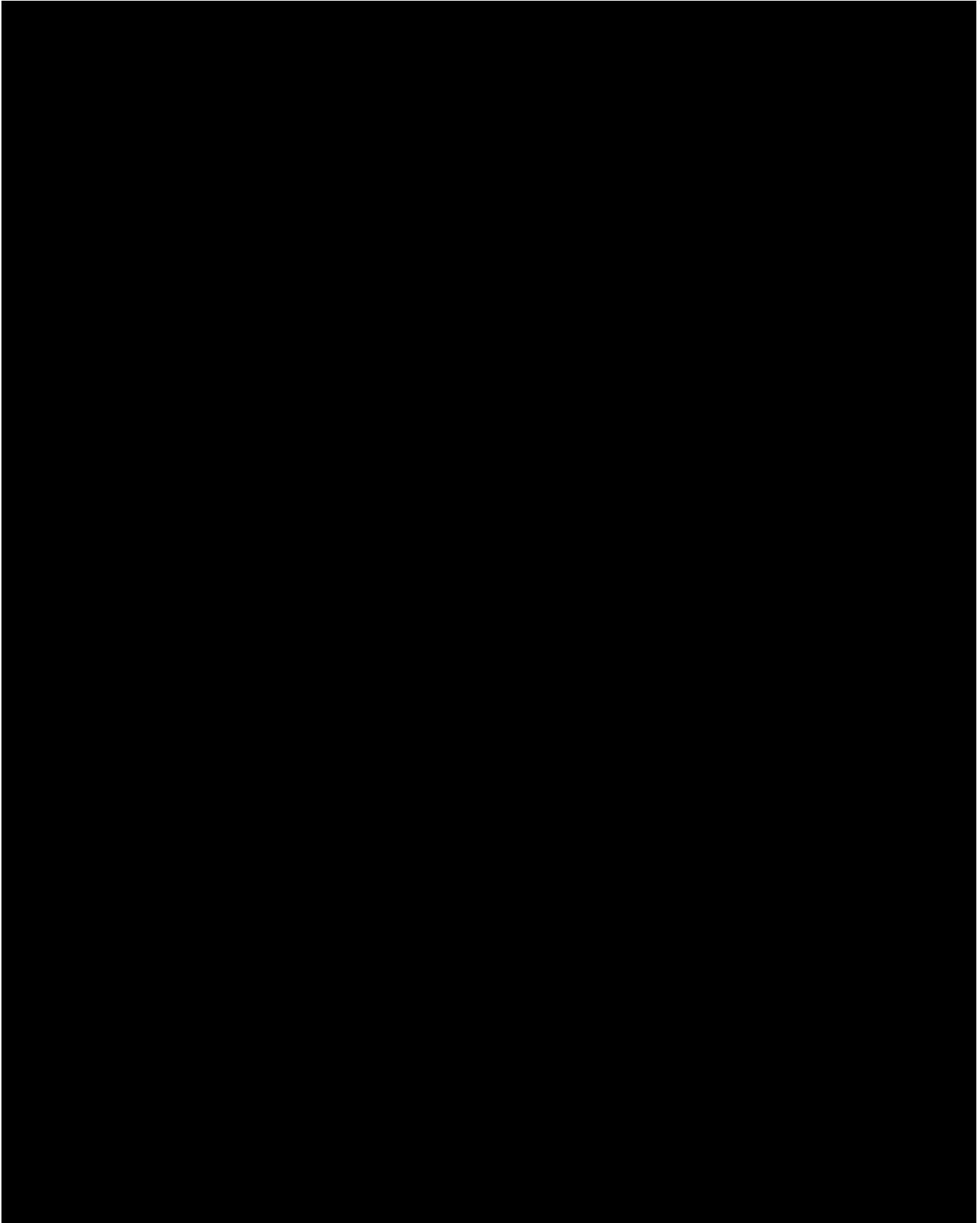
Enter the Installer or Administrator programming. Choose Option 1, then 7. You will be prompted to enter the speed dial number you wish to create/modify. The numbers available are 600-699. Follow the prompts to add or change the name and to enter the number. Be sure to put a 9 before the phone number; this will be needed to pick up a line to make the outgoing call. A list of existing Speed Dial numbers can be found on r:\administrators\phones.

### **When programming feature keys you can use the following Codes:**

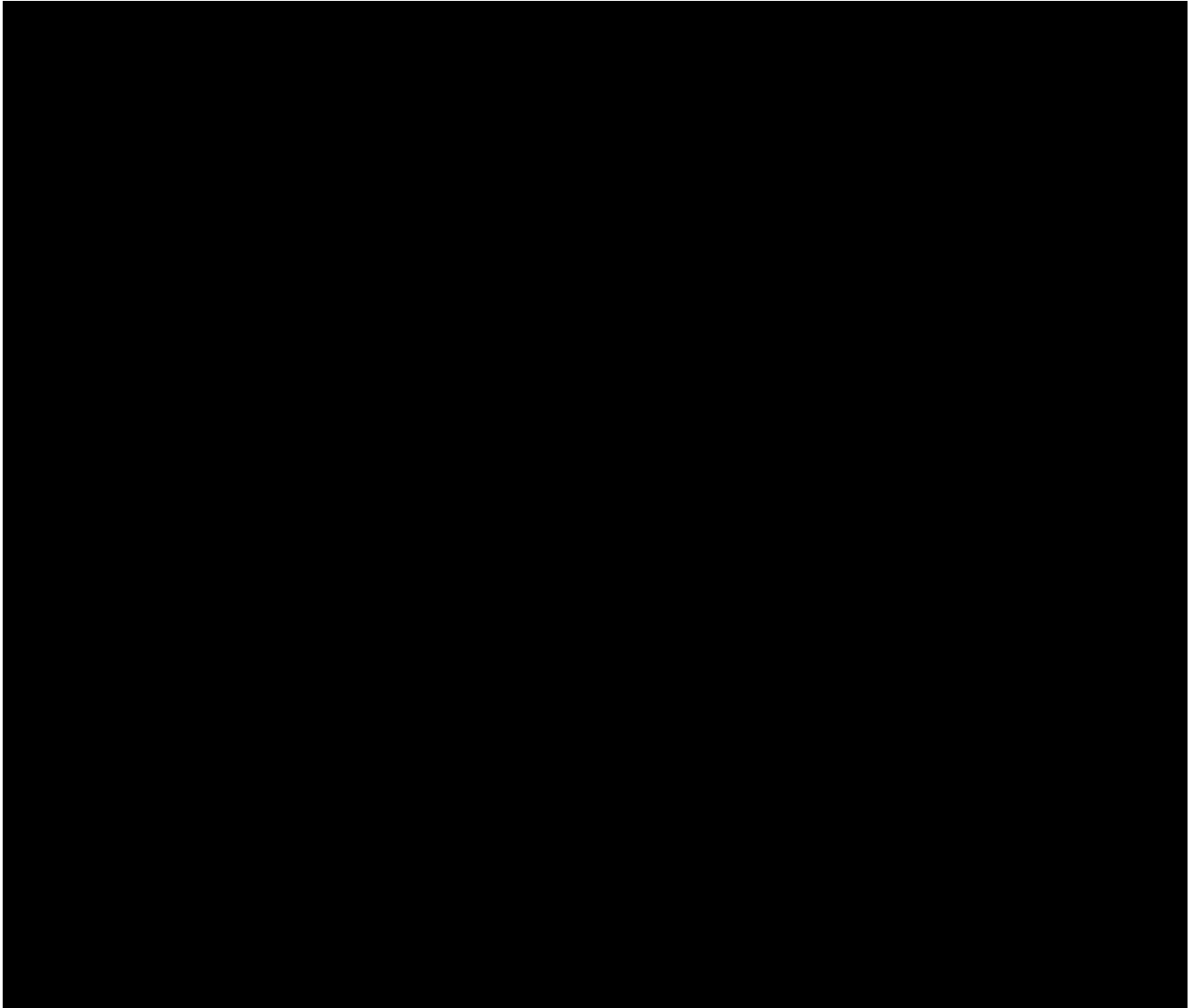
Code(s)	Key usage
199	Overhead page
560	Manual day/night/holiday mode
561	Service observing
5xxx	ACD agent log-on/log-off
562	ACD agent wrap
563XXX	ACD administrator
564	Headset operation
565	Call forward
565YYY	Call forward to specific extension
566	Redial

<b>568</b>	Message monitor key
<b>569</b>	Background announce
<b>570</b>	Conference
<b>571</b>	Personal greeting 1
<b>572</b>	Personal greeting 2
<b>573</b>	Personal greeting 3
<b>574</b>	Missed-Call Key
<b>575, 576</b>	Virtual Answer Keys (available only on 48- and 24-Key Phones)
<b>577</b>	QuickPage
<b>578</b>	Mute/DND
<b>579</b>	Voice mail
<b>580</b>	Override ring

### 7.4.3. Day Mode Diagram - Including Details



#### 7.4.4. Night Mode Diagram



### 7.4.5. Prompt Recordings

#### **Prompts: August 9, 2006**

**ID 1 – Day 1 Mode:** Welcome to JAUNT. You may enter an extension at any time or dial **8** for a Directory of staff. To use our Automated System for checking or canceling your previously scheduled trips, press **1**. To change or schedule a trip for today or for Dispatch, press **2**. To change or schedule a trip for any other day or for Reservations, press **3**. For tickets press **4**. To speak to our receptionist, press **0**. To listen to these options again, press **7**. Thanks a lot for calling JAUNT.

**ID 2 - Night 1 Mode:** Welcome to JAUNT. You may enter an extension at any time or dial **8** for a directory of staff. To use our Automated System for checking or canceling your previously scheduled trips press **1**. To change a trip for Today or for Dispatch, press **2**, for Same-Day trip *Emergencies* **only** when no one is here press **6**, for all other calls, please call back during normal business hours Monday through Friday 8:30 am to 5 pm. And, thank you for calling JAUNT.

**ID 2 - Night 2 Mode:** Welcome to JAUNT. You may enter an extension at any time or press **8** for a directory of staff. For our Automated System for checking or canceling your previously scheduled trips, press **1**. For Same-Day trip *Emergencies* only when no one is here press **6** and you will be transferred to our answering service. For all other calls, please call back during normal business hours Monday through Friday 8:30 am to 5 pm. And thank you for calling JAUNT

**Prompt 538** - Thank you for calling JAUNT, all agents are currently assisting other customers. Please hold for the next available agent. Did you know our Automated system can help you 24 hours a day, ask the Reservationist for more information.

**Prompt 539** - We apologize for the delay, please continue to hold for the next available agent, or if you would like to leave a message, dial 300 now. Did you know our Automated system can help you 24 hours a day, ask the Reservationist or Dispatcher for more information.

**Prompt 540** - Reserved for the Holiday mode and will be used for remotely recording messages to reflect business status in case of severe weather, holidays.

**On Hold Message Source: 592 – Jazz Music**

## Directory Recording – 18, 28

#1 - Enter the first 3 letters of the first name of the person whom you wish to reach.

#2 - When you hear the name of the person you wish to reach, press the pound key and you will be transferred.

## Mailbox Recordings:

**MB 300 (Reservations)** - We're sorry, no one is available to take your call, Did you know our Automated system can help you 24 hours a day, ask the Reservationist for more information. Please leave a message after the tone, Thank you.

**MB 301 (Dispatch)** - We're sorry, no one is available to take your call, Did you know our Automated system can help you 24 hours a day, ask the Dispatcher for more information. Please leave a message after the tone, Thank you.

**MB302** - Thank you for calling about tickets. If you are calling after business hours, please dial 0 now. If you are calling during business hours, please leave a message with your name, phone number and brief message. Thanks, and have a *great* day.

**MB400** – Blank – Used for ad-hoc service changes and downed-system notifications. Plays before system prompt. Typically left blank. Users can not press numbers to be redirected until the system prompt plays after MB400.

## 8. Locations of Important IT Materials:

**ERD/IDR disks** – Located in the server room in a floppy disk case, labeled for each server.

**Software** – Located primarily in Kevan's office on the bookshelf and in the hutch. The right side has server software, the left has PC software. There is also some software in the server room on one of the racks in a CD case. On Kevan's bookshelf is located several CD cases with various software and MS Technet or ([www.microsoft.com/technet](http://www.microsoft.com/technet)).

## 9. Restore Plan

## 10. Power

### 10.1. Battery Backup (UPS)



Uninterrupted Power Supply (UPS) through Battery backups should provide an on going conditioned power source providing an immediate power supply for any power outages, brown-outs or surges. This supply should be sufficient to maintain the system until the generator can take over.

If the server has “Smart” capabilities you can independently configure that server UPS settings. If only Simple Capabilities, they use the default settings for the “Smart” server. The serial cables are special APC cables (wired just for their UPS’s) and must be replaced with same.

**UPS30\_1**, Rack 1, Smart UPS 3000 RM, 3 Serial Interfaces,  
**EJAUNT** - Main Serial Connection – “Smart” Capabilities  
**XGATE** – Interface Expander #1 – Simple Capabilities  
**MAILROOM** - Interface Expander #2 – Simple Capabilities

**UPS14\_1**, Rack 2, Smart UPS 1400 RM, 1 Serial Interface, Environmental Mgt. Card & Sensor  
**MANAGER** – Main Serial Connection – “Smart” Capabilities

**UPS14\_2**, Rack 3, Smart UPS 1400 RM, 3 Interfaces  
**ROOT** – Main Serial Connection – “Smart” Capabilities

**UPS22\_1**, Rack 3, Smart UPS 2200 RM, 3 Interfaces  
**TRAPSOFT** – Main Serial Connection – “Smart” Capabilities  
**MDTAVL** - Interface Expander #1 – Simple Capabilities  
**TRAPDB** - Interface Expander #2 – Simple Capabilities

**UPS22\_2**, Rack 1, Smart UPS 2200 RM  
IVR1 – No software connection with UPS  
IVR2 - No software connection with UPS

## 10.2. Generators – Backup Power

Generators are used to provide longer term power for a limited range of services. They should automatically turn on and switch power over to emergency generator power until utility service is re-enabled. Then the power should be automatically switched off generator power on to utility power. The JAUNT facility generator uses city LP gas for fuel which normally stays active during other outages.

### 10.2.1. Onan 42KW @ JAUNT

**When power goes out for more than 5 seconds the generator will automatically turn on and then switch the emergency circuits over.**

The generator switch box in the telephone closet indicates (round lights) whether or not the electrical service power (Dominion Electric) is working or the generator is on and whether the building is being powered by Dominion Electric or the generator.

There is an enunciator panel above the switch box with several diagnostic lights. If there is a generator malfunction, check and record which lights are blinking or on. Do not open the switch box – that is only for electricians. The generator runs automatically every week. Call the [generator contractor](#), Fidelity Engineering immediately for service.

## 10.2.2. Briggs and Stratton @ Carter Mountain

The generator is designed to be fully automatic and should start well before the backup batteries loose their power. Once per week the generator runs for a few minutes as a test and to keep the unit lubricated.

# 11. Application & Server: Shutdown & Reboot Procedures

## 11.1. Shutdown Procedures

FIRST – shutdown any running applications on the server, watching any log files for “shutdown complete”. Select “Shutdown” from “Start” menu on each server in this order, after closing all open applications (look for open app’s in the task bar at bottom of screen). \*\* Monitor individual shutdowns to ensure power-off sequence occurs in same order for only those noted.

- 11.1.1. EJAUNT
- 11.1.2. MANAGER
- 11.1.3. MDTAVL \*\*
- 11.1.4. TRAPSOFT\*\*
- 11.1.5. TRAPDB\*\*
- 11.1.6. XGATE
- 11.1.7. COMM
- 11.1.8. ROOT
- 11.1.9. IVR1
- 11.1.10. IVR2
- 11.1.11. Tape Backup Unit – ROOT, above ROOT server
- 11.1.12. Tape Backup Unit – MDTAVL & TRAPSOFT

\*\* - these 3 servers are the only ones needing to be in this order. All others can be shut down simultaneously.

11.2. If complete server room shutdown is necessary(Extended power outage);

- 11.2.1. Ensure all units completely shutdown (no sounds or lights)
- 11.2.2. Turn off CISCO PIX unit on center shelf
- 11.2.3. Turn off Battery Backup Systems (UPS) – they will recharge while off

## 11.3. Restart Procedures

Once power has been restored for at least 10 consecutive minutes:

1. Ensure that UPS Battery backup systems indicate at least 4 green LED's in a column on the right side of the unit, and then turn each unit on - if they are off.
2. Make sure each server is *not already booted up* before the pressing power button. Restart each server in this order. **Do not** wait between starting servers (multiple machines can be booting at the same time). Make sure you successfully **log on in order** before logging into the next appropriate server.
  - 2.1. Tape Backup Unit – ROOT, above ROOT server (power button in back, verify green LED light is on)
  - 2.2. Tape Backup Unit – MDTAVL & TRAPSOFT - (power button in back and front, verify green LED light is on)
  - 2.3. ROOT – Should be first to start
  - 2.4. MANAGEMENT – If ROOT cannot start, MANAGER has to, for network to work
  - 2.5. MANAGER
  - 2.6. TRAPDB
  - 2.7. TRAPSOFT – dependant on TRAPDB
  - 2.8. XGATE
  - 2.9. MDTAVL – dependent on XGATE & TRAPSOFT, Make sure Schedule Server app is loaded before MDTAVL app.
  - 2.10. COMM
  - 2.11. IVR1
  - 2.12. IVR2
  - 2.13. EJAUNT

**After rebooting any server** verify there are no error messages (write down wording if there is).

## 11.4. Microsoft Windows 2000/3 – Shutting Down the Server!

In case of an emergency, use the following procedures to shut down a Windows 2000 Server.

From the desktop click **Start**

Click on the **Shutdown...** button.

Choose the **Shutdown** option and click **OK**.

It might take up to 10 minutes or more for the machine to turn off. Do not hard-power off the server unless you are positive it is definitely locked up.

If the message appears, "It is now safe to turn off your computer" press the power button until the server is silent and lights turn off (approx 1 or 2 seconds).

## 11.5. Trapeze Software Shut Down and Restart Procedures

Use the following procedures to shut down and restart the Trapeze Schedule Server Software.

**First –**

- Ensure all Trapeze users throughout building have closed all trapeze apps.
- Shut down MDTAVL server application – see below!! (MDTAVL is dependant upon the SchedSrv Application). While down, vehicles and Dispatch can not send or receive any information.

**Second –**

- Shut down SchedSrv3 application (Yellow Icon) – **Click on SchedSrv3 CDBLOG** file and monitor it until it is “Shut Down”.
- Shut down Trapeze6 Service Shell App (Blue circle w/red/green/yellow balls) CDBLOG should say “Services are shut down”
- Shut down JAUNTIVR Service Shell App (Blue circle w/red/green/yellow balls) CDBLOG should say “Services are shut down”
- Shut down all three CDBLOG files (Blue Eye)

**Third –**

- Restart SchedSrv3 application from TRAPSOFT desktop (Yellow road sign) – **DO NOT START** application twice!!
- Monitor SchedSrv3 CDBLOG file, it should go through several steps including:
  - Load Schedules
  - Load Live Days
  - Error “Fare already collected”
  - Error “Garage not found”
  - Load Beg
  - Load Live End
  - Templates Beginning/End
  - Activate Bookings Begin/End
  - Activate Bookings End
  - Note any additional error messages
- Start Address Matcher from desktop
- Start Info Server from desktop
- Start MDTAVL application – See Below!

## 11.6. MDTAVL Server Application

Use the following procedures to shut down the MDTAVL Server Software. While down, vehicles and Dispatch can not send or receive any information. TRAPSOFT must be up and running for this application to operate properly.

The Task bar should contain the MDTSRV.JAUNT application icon (grey box w/green lines) and MdtSrv2 CDBLOG (Eye)

1. From the desktop select the MDTSRV.JAUNT (grey box w/green lines) Application Software and close that window.
2. Select the CDBLOG and wait until the log shows the application is closed or two minutes
3. Then close the CDBLOG window

**TO RESTART APPLICATION** – after both the application and logs are closed

Find the Grey Box with Green lines icon on the desktop (MDT Server MSrv41\_2.exe) and double click (BE PATIENT, DO NOT OPEN IT TWICE)

Immediately click on the CDBLOG and look for any red colored errors

Report any red errors to Kevan or Trapeze Customer Care Center

## 11.7. XGATE Server Application

In case of an emergency, use the following procedures to shut down the XGATE Server Software. Rebooting the application should not affect the drivers if it is started back up directly afterwards.

The Task bar should contain the XGATE application icon (if not, application has crashed, proceed to Restarting application)

From the desktop select the XGATE Application Software and close the window

**TO RESTART APPLICATION**

- Find the Black and Red “X” icon on the desktop (XGATE 3.x) and double click (BE PATIENT, DO NOT OPEN IT TWICE) If two buttons appear on task bar, Close both and carefully open it again.
- Look at the “Link Summary” – “Dispatch” “Status” should read “Connected to 192.168.169.226” give it a couple of minutes to check link status. [Other two Links (Down) are NOT used – Disregard] If it does not connect, check MDTAVL server and verify MDTServ application is running properly
- “Channel Summary” should state “Connected to MCC at 9600 bps” If not, connection with tower broken. Check Modem and ensure it reads
- Event Summary - Look at Date and Time should not show “Purging inbound status ‘Because status link is Down’ for current date/time – if it does contact Mentor Engineering
- System Information – should indicate Database: JAUNT on XGATE, CPU Info: XGATE :: 192.168.169.227
- In the lower right corner of the desktop, look for a grey icon in the shape of a computer with a circle next to it – The circle should contain a green arrow, *if it is red*, right click the icon and select MSSQLServer – Start. Within three minutes a green arrow should appear. If not contact Mentor.

## 12. Documentation

### 12.1. Acceptable Use of Jaunt's Information Systems Policy

# Acceptable Use of JAUNT's Information Systems

## General Principles

Information maintained by JAUNT is a vital asset that will be available to all employees who have a legitimate need for it, consistent with JAUNT's responsibility to preserve and protect such information by all appropriate means.

By definition, "Information Systems" include, but are not limited to, PCs and all associated hardware, telecommunications equipment (telephones, cell phones, pagers, two-way radios, etc.), copiers, fax machines, printers, laptops, Mobile Data Computers (MDC), cameras, scanners, audio/visual equipment, JAUNT- authorized software and all network-related resources.

Access to information systems and networks owned or operated by JAUNT, Inc. imposes certain responsibilities and obligations and is granted subject to local, state, and federal laws. Acceptable use is ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. Pre-authorized personal use of information systems must not interfere with work hours.

## Guidelines

In making acceptable use of resources you must:

- use resources only for authorized purposes.
- protect your username and system from unauthorized use. You are responsible for all activities with your username or that originate from your system while you are logged on. Do not share your password with anyone other than IT staff, unless properly authorized. If you must reveal your password, notify an IT staff member and request a new password immediately.
- access only information that is your own, that is publicly available, or to which you have been given authorized access.
- inform IT staff and/or senior staff if you are exposed to information you deem offensive, intimidating or otherwise inappropriate to the work environment.
- notify IT staff and/or senior staff if you have access to information that you feel might be inappropriate or unnecessary in the scope of your authorized duties.
- keep all private information confidential.
- use only legal versions of copyrighted software in compliance with vendor license requirements.
- provide IT staff with any JAUNT- authorized software disks and documentation.
- be considerate in your use of shared resources. Do not monopolize shared computers, transmit or invite excessive data over the network, or degrade services; do not waste disk space, printer paper, manuals, or other resources.
- Use appropriate methods of transferring confidential or sensitive information.

In making acceptable use of resources you must **NOT**:

- use JAUNT's information systems for personal gain.
- use another person's username, password, files, or data without appropriate authorization.
- allow any non-authorized person to use JAUNT information systems including connecting non-authorized equipment to them.
- use computer programs to decode passwords, access system or control information.
- attempt to avoid or undermine system or network security measures.
- purposefully engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to JAUNT data.
- use JAUNT systems for any political or religious causes, such as using electronic mail to circulate advertising for products or for or against political candidates, etc.
- represent JAUNT, Inc. electronically (via email, fax, etc.) unless you are authorized to do so.
- install *any* software without proper authorization, including downloaded programs from Internet.
- make or use illegal copies of copyrighted software, store such copies on JAUNT systems, or transmit them over the JAUNT network.
- use information systems to display or transmit any material that could be construed as creating a hostile work environment, including sexually explicit or obscene images, messages, cartoons, or ethnic slurs, racial epithets, or anything that could be construed as harassment or disparagement of others based on their race, color, national origin, sex, age, disability, or religious or political beliefs.
- waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, broadcasting unsolicited messages, printing excessive amounts of paper, or by sending/forwarding chain letters or unsolicited mass mailings.
- use JAUNT's systems or networks for personal gain; for example, by selling access to your username or to JAUNT systems or networks, or by performing work for profit with JAUNT resources in a manner not authorized by JAUNT.
- engage in any other activity that does not comply with the General Principles represented above

## **Implementation**

JAUNT considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information from JAUNT systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten security or degrade operations. Violators are subject to disciplinary action. Offenders also may be prosecuted under laws including (but not limited to) the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, The Virginia Computer Crimes Act, and the Electronic Communications Privacy Act. JAUNT also reserves the right to monitor the use of JAUNT's technology. Employees are responsible for any charges incurred in their personal use of JAUNT's information systems.

## 12.2. Web Site Privacy Statement

### 12.2.1. "Customer Identifiable" Information

Protecting one's privacy is of paramount importance to JAUNT. JAUNT has developed a policy recognizing and protecting the privacy of customers and general public who browse JAUNT's [www.ridejaunt.org](http://www.ridejaunt.org) web site for information. The company maintains strict information privacy policies and uses appropriate technologies to safeguard such information from unauthorized intrusions.

JAUNT acknowledges that the growth of online services, including Internet services, has created additional privacy concerns, especially for customers.

Such concerns primarily focus on the protection of "customer identifiable" information which individuals reasonably expect to be kept private. "Customer identifiable" information is that information which can be associated with a specific individual or entity (for example, a customer's name, address or telephone number, E-mail address and certain information about online activities that are directly linked to them).

Commonly, it is necessary for companies, governmental agencies, or other organizations to collect "customer identifiable" information in order to conduct business and provide services. (For example, JAUNT may collect "customer identifiable" information, such as name, address, telephone number, etc., in the course of responding to customer inquiries about its services.)

### 12.2.2. JAUNT Online Privacy Policy

JAUNT has established the following JAUNT Web site Privacy Policy to protect "customer identifiable" information. The policy covers JAUNT, its subsidiaries and affiliates and applies to all customer identifiable information that JAUNT gathers when a customer uses a JAUNT online web site (JAUNT web site). It is JAUNT's intention to continue to protect "customer identifiable" information consistent with applicable federal, state and local laws.

### 12.2.3. JAUNT Protects Online "Customer Identifiable" Information as follows:

**Disclosure.** JAUNT will not sell, trade, or disclose to third parties any "customer identifiable" information derived from a customer's use of a JAUNT web site without the consent of the person, as the case may be (except as may be legally required or in the case of imminent physical harm to the customer or others). Also, when JAUNT utilizes other agents, contractors or companies to perform services on its behalf, JAUNT will ensure that the company or agent will protect your "customer identifiable" information consistent with this Policy.

**Collection & Use.** JAUNT will collect and use "customer identifiable" information for billing purposes, to anticipate and resolve problems with services or possibly to create and inform you of products and services that better meet your needs. While JAUNT may use your "customer identifiable" information, together with information obtained via other sources, to improve services which JAUNT considers may be of interest to you, JAUNT will not disclose your "customer identifiable" information to third parties who may want to market to you.

## 12.3. IP Address Schemes

**Internal Network:** 192.168.169.0/255.255.255.0

**DMZ** 192.168.168.0/255.255.255.0

**External Network:** 12.5.57.0/255.255.255.224



## 12.3.1. Internal IP's

COMM .120  
MANAGEMENT .121 .122  
Mailroom/Dns 192.168.169.220  
Trapsoft/ 192.168.169.221  
Trapdb/SQL 192.168.169.222  
ejaunt/web ridejaunt.org 192.168.168.223  
ejaunt/web ctav.org 192.168.168.224  
Root/Dns 192.168.169.225  
Mdtavl 192.168.169.226  
Xgate 192.168.169.227  
Manager 192.168.169.228  
IVR1 .229  
IVR2 .230  
faxcanon .231  
Gateway/PI X 192.168.169.1

business office-Laser 192.168.169.75  
reservations laser .76  
receptionist laser .77  
HP fax/ptr/scan machine D155xi .78  
HPLJ 4300 tn .79  
ADMIN HP4350 Reception .82  
Ricoh/ICON Copier/Printer/Fax/Scanner .83  
Netgear Wireless Access Point .84

Dhcp-PC's .2 - .55  
Latitude laptop .56

3COM old 3300 Switches .97(MM), .98(XM), .99(XM)  
New  
3870 bottom svr rm (GBIT) 100  
21 & 22 1000 link to .101  
24 fiber link to LIU/1st flr closet

4228G middle svr rm. 101  
25/Up conn to .100-22  
26/Down conn to .100-21

4228G top svr rm .102  
28 fiber link to .100-21  
25/Up conn to .100-23  
26/Down conn to .100-24

4228G 1st flr closet .103  
27 fiber conn to LIU MDF-1 to .100-24

28 fiber conn to LI U MDF-1 to 2nd flr LI U to .104-27

4228G 2nd flr .104

27 fiber conn to LI U-MDF-02/1st flr

4228G middle svr rm. .105

ESI PHONE PBX IP - .106

esi installer password 3822 8822

VPN Group (PI X) .150 - .155

DRAC - Dell Remote Access Card

trapsoft .67

trapdb .66

xgate .68

mdtavl .69

root .70

COMM .218

Open Manage DHCP Scope:

.61-.65

APC NETWK CARDS

UPS30-1 .80

UPS 22-1 .81

### 12.3.2. External IP's

MX - mail.ridejaunt.org 12.5.57.98

Web - ridejaunt.org and www.ridejaunt.org 12.5.57.100

Ftp - ftp.ridejaunt.org 12.5.57.100

Web - ctav.org and www.ctav.org 12.5.57.110

Ftp - ftp.ctav.org 12.5.57.110

PIX IP Address outside 12.5.57.126

Global outside 12.5.57.116-124 pool for getting out.

PIX Route - XGATE 12.5.57.115 for ports 5631 and 5632 from host 68.145.8.246

to Server 192.168.169.227 for mentor direct connect

new

12.5.57.113 to 192.168.169.130 for 146.82.184.3 LogicTree Access

12.5.57.114 to 192.168.169.229 for 146.82.184.2 LogicTree Access

12.4.199.56/30 connectivity from Wahoo

BNSI Cisco 1600 Router 12.5.57.97

12.5.57.96/27 IPs for Jaunts use

range of usables: 12.5.57.98 to 12.5.57.126

subnet mask: 255.255.255.224

### **BNSI External DNS for JAUNT:**

12.5.48.2-esinet1.esinet.net/ns1.esinet.net

12.5.48.4-esinet2.esinet.net/ns2.esinet.net

198.137.202.3-Limpia.KJSL.COM /ns.kjsl.com

## **12.4. Jaunt Phone Lines**

### **\*Rollover Group**

Rollover Group#1 (6174) (3184)

(1) 296-6174 - Main billing #

(2) 296-6175

(3) 296-8413

(4) 296-0160 security call out

(5) 296-3184

(6) 296-4980

(7) 984-6058

(8) 296-0514 -local conn to toll free# 800-365-2868

(9) 296-0730 Sprint old modem #

Non-rollover

(10) 220-2537

296-1391 sprint new modem/cordless

296-8861 Sprint Analog line for HVAC modem/Southern Air

fax 296-4269 Intelos

Nelson cell 996-6381/2???

Mike & Eugenew

Barbara cell 996-3137

Eugene cell 996-3227

Crystal?996-6381

\* - All incoming calls rollover to subsequent #...throughout all lines regardless of group until open line is found else, caller gets a busy signal

## **13. System Disaster Recovery and Preparation**

from Chapter 14, Microsoft Windows 2000 Administrator's Pocket Consultant by William R. Stanek. ON KEVAN'S BOOKSHELF!!

Backups are only one part of a comprehensive disaster recovery plan. You also need to have Emergency Repair disks and Boot disks on hand to ensure that you can recover systems in a wide variety of situations. You may also need to install the Recovery Console.

## 13.1. Setting Out to Recover a System:

- 13.1.1. Try to start the system in Safe Mode, as described in the section of this chapter entitled "Starting a System in Safe Mode."
- 13.1.2. Try to recover the system using the Emergency Repair disk (if available). See the section of this chapter entitled "Using the Emergency Repair Disk to Recover a System."
- 13.1.3. Try to recover the system using the Recovery Console. See the section of this chapter entitled "Working with the Recovery Console."
- 13.1.4. Restore the system from backup. Be sure to restore the system state data as well as any essential files.

## 13.2. Emergency Repair Disk/Automated Recovery System

The Emergency Repair disk can often help you recover a system that won't boot. This disk stores the essential system files, partition boot sector, and startup environment for a particular system. You should create a repair disk for each computer on the network, starting with Windows 2000 servers. Normally, you'll want to update this disk when you install service packs, manipulate the boot drive, or modify the startup environment.

Tip When you completed the installation of the operating system, basic recovery information was saved in the %SystemRoot%\Repair folder on the system partition. The Repair folder contains a copy of the local Security Account Manager (SAM) data and other essential system files. It doesn't contain a backup of the Windows registry. You should create a registry backup when you create the Emergency Repair disk.

You can create an Emergency Repair disk by completing the following steps:

1. Start Backup. In the Welcome tab, click Emergency Repair Disk.
2. When prompted as shown in Figure 14-9, insert a blank 3.5-inch, 1.44-MB disk into the floppy drive.

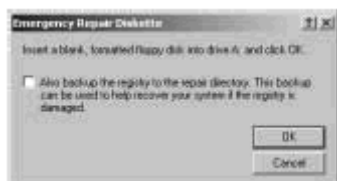


Figure 14-9 Insert a blank disk at prompt. You can also back up the registry.

- Select "Also Backup The Registry To The Repair Directory". A backup of the Windows registry will then be made in the %SystemRoot%\Repair folder. If you need to restore the registry, you must use the Recovery Console.
- Click OK. When prompted, remove the disk and label it as an emergency repair disk for the system.

## 13.3. Creating Setup Boot Disks

You should create boot disks for each version of Windows 2000 running on the network. For example, if you're running Windows 2000 Professional and Windows 2000 Server, you should create boot disks for both of these versions. You use the boot disks to start a system that won't boot so that you can use the Emergency Repair disk or the Recovery Console to fix the system.

**Note** If all of your computers can boot from CD-ROM, you don't need the setup boot disks. Just insert the Windows 2000 CD-ROM when starting the system.

To create boot disks, follow these steps:

1. Insert the Windows 2000 CD into the CD-ROM drive.
2. Click the Start menu, and then click Run.
3. In the Run dialog box, type `h:\bootdisk\makeboot a:` where `h` is the CD-ROM drive letter and `a:` is the floppy drive letter. Click OK.
4. You'll need four blank disks. When prompted, insert a blank 3.5-inch, 1.44-MB disk. Then press any key.
5. When prompted, remove the disk and label it as 1 of 4. Repeat this procedure for the remaining disks.

## 13.4. Starting a System In Safe Mode

If a system won't boot normally, you can use Safe Mode to recover or troubleshoot system problems. In Safe Mode, Windows 2000 loads only basic files, services, and drivers. The drivers loaded include the mouse, monitor, keyboard, mass storage, and base video. No networking services or drivers are started—unless you choose the Safe Mode With Networking option. Because Safe Mode loads a limited set of configuration information, it can help you troubleshoot problems. In most cases, you'll want to use Safe Mode before trying to use the Emergency Repair disk or the Recovery Console.

You start a system in Safe Mode by completing the following steps:

1. Start (or restart) the problem server.
2. During startup you should see a prompt labeled Please Select The Operating System To Start. Press F8.
3. Use the arrow keys to select the Safe Mode you want to use, and then press Enter. The Safe Mode option you use depends on the type of problem you're experiencing. The key options you may see are
  - o Safe Mode Loads only basic files, services, and drivers during the initialization sequence. The drivers loaded include the mouse, monitor, keyboard, mass storage, and base video. No networking services or drivers are started.
  - o Safe Mode With Command Prompt Loads basic files, services, and drivers, and then starts a command prompt instead of the Windows 2000 graphical interface. No networking services or drivers are started.
  - o Safe Mode With Networking Loads basic files, services, and drivers, as well as services and drivers needed to start networking.
  - o Enable Boot Logging Allows you to create a record of all startup events in a boot log.

- o Enable VGA Mode Allows you to start the system in Video Graphics Adapter (VGA) mode, which is useful if the system display is set to a mode that can't be used with the current monitor.
- o Last Known Good Configuration Starts the computer in Safe Mode using registry information that Windows 2000 saved at the last shutdown.
- o Directory Services Recovery Mode Starts the system in Safe Mode and allows you to restore the directory service. Option available on Windows 2000 domain controllers.
- o Debugging Mode Starts the system in debugging mode, which is only useful for troubleshooting operating system bugs.

If a problem doesn't reappear when you start in Safe Mode, you can eliminate the default settings and basic device drivers as possible causes. If a newly added device or updated driver is causing problems, you can use Safe Mode to remove the device or reverse the update.

## 13.5. Using The ER Disk To Recover a System

When you can't start or recover a system in Safe Mode, your next step is to try to recover the system using the Emergency Repair disk. This disk comes in handy in two situations. If the boot sector or essential system files are damaged, you may be able to use the repair disk to recover the system. If the startup environment is causing problems on a dual or multi-boot system, you may be able to recover the system as well. You can't recover a damaged registry, however. To do that, you must use the Recovery Console.

You can repair a system using the Emergency Repair disk by completing the following steps:

- Insert the Windows 2000 CD or the first setup boot disk into the appropriate drive, and then restart the computer. When booting from a floppy disk, you'll need to remove and insert disks when prompted.
- If repairing a Windows 2000 server, PRESS F6 in the beginning of the blue screen when it specifies at the bottom of the screen. You only have approximately 5 seconds to press F6 so you have to pay attention.
- When the Setup program begins, follow the prompts, and then choose the Repair or Recover option by pressing R.
- Choose emergency repair by pressing R, and then do one of the following:
  - o Press M For Manual Repair Select this option to choose whether you want to repair system files, the partition boot sector, or the startup environment. Only advanced users or administrators should use this option.
  - o Press F For Fast Repair Select this option to have Windows 2000 attempt to repair problems related to system files, the partition boot sector, and the startup environment. This option runs all repair options.
- Insert the Emergency Repair disk when prompted. Damaged or missing files are replaced with files from the Windows 2000 CD or from the %SystemRoot%\Repair folder on the system partition. These replacement files will not reflect any configuration changes made after setup, and you may need to reinstall service packs and other updates.
- If the repair is successful, the system is restarted and should boot normally. If you still have problems, you may need to use the Recovery Console.

## 13.6. Working With the Recovery Console

The Recovery Console is one of your last lines of defense in recovering a system. The Recovery Console operates much like the command prompt and is ideally suited to resolving problems with files, drivers, and services. Using the Recovery

Console, you can fix the boot sector and master boot record; enable and disable device drivers and services; change the attributes of files on FAT (file allocation table), FAT32, and NTFS volumes; read and write files on FAT, FAT32, and NTFS volumes; copy files from floppy or CD to hard disk drives; and run check disk and format drives.

The sections that follow discuss techniques you can use to work with the Recovery Console. As you'll learn, you can start the Recovery Console from the setup boot disks or you can install the Recovery Console as a startup option.

## 13.7. Installing the Recovery Console as a Startup Option

On a system with frequent or recurring problems, you may want to install the Recovery Console as a startup option. In this way, you don't have to go through the setup boot disks to access the Recovery Console. You can only use this option if the system is running. If you can't start the system, see the section of this chapter entitled "Starting the Recovery Console."

You install the Recovery Console as a startup option by completing the following steps:

1. Insert the Windows 2000 CD into the CD-ROM drive.
2. Click the Start menu, and then click Run. This displays the Run dialog box.
3. Type `h:\i386\winnt32.exe /cmdcons` in the Open field, where `h` is the CD-ROM drive letter.
4. Click OK, and then when prompted, click Yes. The Recovery Console is then installed as a startup option.

Note Normally, only administrators can install and run the Recovery Console. If you want normal users to be able to run the Recovery Console, you must enable the Auto Admin Logon policy for the local computer policy (Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/Auto Admin Logon).

## 13.8. Starting the Recovery Console

If a computer won't start and you haven't installed the Recovery Console as a startup option, you can start the computer and the Recovery Console by completing the following steps:

- 15..8.1 Insert the Windows 2000 CD or the first setup boot disk into the appropriate drive, and then restart the computer. When booting from a floppy disk, you'll need to remove and insert disks when prompted.
- 15..8.1 When the Setup program begins, follow the prompts, and then choose the Repair Or Recover option by pressing `R`.
- 15..8.1 If you haven't already done so, insert the Windows 2000 CD into the appropriate drive when prompted.
- 15..8.1 Choose Recovery Console by pressing `C`. When prompted, type the local administrator password.
- 15..8.1 When the system starts, you'll see a command prompt into which you can type Recovery Console commands. Exit the console and restart the computer by typing `exit`.

## 15.9 Recovery Console Commands

The Recovery Console is run in a special command prompt. At this command prompt, you can use any of the commands summarized in Table 14-5.

**Table - Recovery Console Commands**

Command	Description
ATTRIB	Changes the attributes of a file or directory.
BATCH	Executes a series of commands set in a text file.
CD	Changes the current directory.
CHKDSK	Runs the Chkdsk utility to check the integrity of a disk.
CLS	Clears the screen.
COPY	Copies a single file to another location.
DEL	Deletes one or more files.
DIR	Displays a directory listing.
DISABLE	Disables a system service or a device driver.
DISKPART	Manages partitions on hard disk drives.
ENABLE	Starts or enables a system service or a device driver.
EXIT	Exits the Recovery Console and restarts your computer.
EXPAND	Expands a compressed file.
FIXBOOT	Writes a new partition boot sector.
FIXMBR	Repairs the master boot record.
FORMAT	Formats a disk.
HELP	Displays a list of Recovery Console commands.
LISTSVC	Lists the services and drivers available on the computer.
LOGON	Logs on to a Windows 2000 installation.
MAP	Displays drive letter mappings.
MD	Creates a directory.
MORE	Displays a text file one page at a time.
REN	Renames a single file.
RD	Removes a directory.
SET	Displays and sets environment variables.
SYSTEMROOT	Changes to the systemroot directory.
TYPE	Displays a text file.



## 15.10. Deleting the Recovery Console

If you installed Recovery Console as a startup option and no longer want this option to be available, you can delete the Recovery Console. To do that, follow these steps:

1. Start Windows Explorer, and then select the hard disk drive on which you installed the Recovery Console. This is normally the boot drive.
2. From the Tools menu, select Folder Options.
3. In the View tab, select Show Hidden Files And Folders, and then clear the Hide Protected Operating System Files check box. Click OK.
4. The right pane should show the root directory for the boot drive. Delete the Cmdcons folder and the Cmlldr file.
5. Right-click the Boot.ini file, and then click Properties.
6. In the Properties dialog box, clear the Read-Only check box. Then click OK.
7. Open Boot.ini in Notepad. Then remove the startup entry for the Recovery Console. The entry looks like this:

```
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000 Recovery Console" /cmdcons
```

8. Save the Boot.ini file, and then change its property settings back to read-only.

Once deleted, the Recovery Console is no longer listed as a startup option. You can reinstall the console if you need to at a later date or run the console as described in the "Starting the Recovery Console" section of this chapter.